Testimony of

Benjamin G. S. Fowke III

Chairman of the Board, President & Chief Executive Officer

Xcel Energy Inc.

before the

U.S. Senate Committee on Energy & Natural Resources

Subcommittee on Energy

hearing to

Examine Cybersecurity Threats to the US Electrical Grid and Technology Advancements to Minimize the Threat

Chairman Gardner, Ranking Member Manchin, and members of the Subcommittee, thank you for the invitation to speak at this important hearing.

My name is Ben Fowke, and I am the CEO of Xcel Energy, an integrated energy company serving 3.5 million electric customers and 2 million natural gas customers. Headquartered in Minneapolis, we serve parts of eight Western and Midwestern states, including the Twin Cities of Minnesota, Denver and the Colorado Front Range, and the Texas Panhandle. We have a balanced energy mix that includes natural gas, coal, nuclear and renewables. We are also the nation's No. 1 utility wind energy provider with more than 8,000 megawatts on our system.

I am pleased to join you today to discuss the critical issue of cybersecurity and the potential threat to the electric grid. As a CEO of a major electricity supplier, one of my highest priorities is protecting Xcel Energy's customers from loss of electric service due to this growing threat. In conjunction with this priority, I have also joined with leaders in the electric sector, government and other lifeline sectors to help develop national programs and strategies to promote the protection of the nation's critical infrastructure. I am a member of the Electric Sector Coordinating Council, or ESCC, which serves as the principle liaison between the federal government and the electric power sector. I am also a member of the National Infrastructure Advisory Council, or NIAC, where I join with other leaders in the private sector to advise the President on ways that the nation can protect its critical infrastructure.

Xcel Energy and the utility industry recognize the significant threat associated with cybersecurity. Our modern society depends on electricity – and left unprotected, the grid and the reliability of electric service that we all depend on would be at risk. Fortunately, as I will discuss today, Xcel Energy and other utilities have developed cybersecurity systems and programs designed to adapt and respond to the evolving cyber threat. While no program is perfect, and constant vigilance is critical, I believe that our industry's approach should give our customers, the subcommittee and the American public increased confidence in the security of the electric grid.

That confidence, however, should be seen in the context of the significance of the challenge before us. Attacks on our grid continue to grow in number and sophistication. We in the industry have a responsibility to meet this mutating threat, but we need support from Congress and our federal partners. As my testimony indicates, we need better coordination with the Department of Energy, Department of Homeland Security and other agencies. We need better, more timely and efficient information sharing (including machine-to-machine information sharing technologies), and quicker dissemination of classified information regarding security threats. We need new research into technologies and strategies to protect the grid, including the technologies embedded in the operational devices that run our electric systems. Together, these strategies and the others I discuss today will enhance and maintain our cybersecurity defenses and help enhance the reliability of the electric grid.

The Cyber Threat to the Grid is Growing.

Like virtually every company in America, Xcel Energy is subject to a growing cyber threat. In 2016, Xcel Energy identified over 500,000 individual cyber attacks on our network. We are attacked daily, and, each year, the number of attempted intrusions grows. In the first quarter of this year, we have seen a 10% increase in the attacks against our network and systems since the prior year.

Most cyberattacks against a utility are similar to the attacks targeting any other company. These attacks seek personal or corporate data, attempt to defraud the company or its customers or hold the company's network hostage in a "ransomware" attack. While attacks from cybercriminals and "hacktivists" can do much damage to any company, utilities like Xcel Energy have an even greater concern, the same concern that prompted today's hearing: attacks from terrorists or nation-states targeting the control systems for the electric grid.

Most electric grids are controlled by industrial control systems, often called "Energy Management Systems" or the "Supervisory Control and Data Acquisition," or "SCADA" system. A SCADA system allows utility operators to control the flow of power efficiently to maintain reliable, low priced electric service. Using digital communication and control technology, a

SCADA system gives operators the ability to monitor power flows and voltage and adjust system resources to minimize electric service interruptions.

SCADA systems are used to control both the bulk electric system, i.e. the high voltage transmission system that delivers power to multiple communities across a wide geographic area, and the local distribution system. SCADA can open or close breakers, activate electric generation, shed load and take other steps to protect the grid from outages. SCADA systems for one utility or region are interconnected to other utilities or regions, helping to maintain electric reliability across broad swaths of the country. Modern electricity operations would be greatly impaired without SCADA.

Unfortunately, the convenience and efficiency of SCADA systems also leaves them vulnerable to cyberattack. SCADA uses digital communication and control, and, like anything that uses digital technology, it can be hacked without proper controls and vigilant monitoring. A cyberattack of the SCADA system could allow a third party to override the operator's control of the electric system and take malicious actions designed to prevent the delivery of power to customers. This subcommittee is aware of the attack on the Ukrainian electric system, which showed one possible pathway for the use of cyber tools to disrupt electric operation. The Ukrainian attack was the result of a chain of events that could have been disrupted had the Ukrainian utilities used many of the cybersecurity programs I will describe today. However, the success of the attack demonstrates that such an attack is possible in North America and confirms the need for grid operators to be vigilant.

Cybercriminals can gain this kind of control through several strategies, many surprisingly simple. They may simply steal or guess an operator's password. They may use "phishing" – emails that include malware that, once opened by the recipient, will download a file onto the system that allows access to the network, potentially to gain access to or control of the SCADA system. They may spread malware through "watering holes," i.e. compromised websites or ad content on legitimate sites. They may imbed malware in physical devices that are installed in the SCADA system or elsewhere on the grid and download their malware automatically into the control software of the SCADA. They may interfere with the SCADA system control and communication through a denial of service attack that overwhelms the system with information unrelated to its operation. Without appropriate monitoring, controls and response (such as I will describe shortly), these different avenues of attack would leave the system vulnerable.

As I previously indicated, most cyberattacks originate from cyber criminals interested in stealing information or dollars or "hacktivists" with a political agenda. Attacks on industrial control systems are different; we believe that the majority of these attacks originate from nation-states or from terrorist organizations who intend harm to America's national security. Because of the challenge of assigning attribution to cyberattacks, it is difficult for Xcel Energy to identify the origin of most attacks against our system.

Xcel Energy is Committed to Creating Robust Programs to Help Defend Against Cyberattacks.

The cybersecurity threat is evolving. Fortunately, up to this point, we are not aware of any successful attack on the American electric system, but the risk is clearly growing. In response, we work continuously to implement a flexible, effective cybersecurity program that proactively adapts our cyber defenses to the rapidly evolving threat before an attack occurs.

Like other utilities, we based our cybersecurity program on the "Dynamic Defense in Depth" cybersecurity framework published by the National Institute of Standards and Technology, or NIST. That framework contains several elements:

- Identify. The NIST Cybersecurity Framework first identifies the potential cyber threats and their impact on our business processes. For a utility, this element focuses on the SCADA system and the threats that I previously identified.

- Protect. The NIST framework creates evolving protections for critical infrastructure, including the electric system and especially the SCADA system. For Xcel Energy, our program separates the SCADA system from the rest of our network and from the internet – a separation known as "enclaving." Enclaving places these systems in a tightly controlled and monitored segment of the network, separate from the rest of the company's IT network and the internet. We employ multiple layers of security controls at the perimeters of these enclaves designed to prevent, detect and respond to unauthorized access attempts. We promote good cyber hygiene by promptly and regularly applying appropriate security patches to vulnerable systems, and strictly controlling and monitoring employee access to our critical systems, particularly those within the SCADA system. We have controls in place designed to mitigate the threat of malicious insiders such as banning the use of thumb drives and other removable media, physical access controls and other measures. We also employ two-factor authentication for our SCADA system, requiring passwords and security codes from two different sources before allowing access.

- Detect. Detection is a key component of the NIST framework. Our network is monitored by a dedicated team of cyber analysts on a 24 hour basis. Collecting data from tens of thousands of systems across the network, the team evaluates millions of individual "events" daily in order to identify and respond to unusual or suspicious activity. We receive prompt and actionable threat intelligence daily from government and private sources regarding potential attacks, malware types and methodologies, and we use this intelligence to adjust our defense posture as necessary. Our program uses this information to detect vulnerabilities in our system before the cybercriminal can exploit them. This element is especially important; in most recent high-profile attacks by nation-states, malware sat undetected in the victim's cyber system for months or years before it was exploited. (This type of malware is known as an Advanced Persistent Threat, or

APT, and it allows an actor to gain a foothold in the network for future attacks.) We also employ a vigorous threat detection program that scans the entire network for vulnerabilities or potential changes to our systems that may indicate a compromise.

- Respond. The NIST framework also requires effective response to cyberattacks. Our program isolates and removes detected malware. We maintain up-to-date patching of our system and implement anti-virus, anti-malware programs to address known and unknown threats. However, because there are an increasing number of previously unknown vulnerabilities, referred to as Zero Day Threats, we cannot rely solely on these controls to detect and counter intrusions into our network. We also "hunt" for indications of compromise on regular basis in order to detect and eliminate APTs. Finally, we perform penetration testing of the network by qualified third parties and select government labs and agencies.

- Recover. Unfortunately, despite our best efforts, no program is perfect. Eventually, an attack against our network or even the SCADA system may be successful. The NIST framework recognizes this fact. Accordingly, we maintain highly detailed incident response and recovery plans, both for prompt restoration of system operations and isolation and elimination of the cyber threat. These plans include development of the capability to run the grid without the SCADA system on a short term basis and participation in cyber mutual assurance and other programs in coordination with the ESCC. To test these plans, we join in multiple annual local, state and national level exercises, such as GridEx. I will discuss these programs and exercises in more detail later in this testimony.

  In fact, system recovery is one of our highest priorities. From the beginning, utilities have had to face threats to their system reliability, including storms, fires, and equipment failures. We have decades of experience bringing our system back from unforeseen outages. While the challenges of system restoration would be different after a cyberattack, our experience with system restoration gives us a leg up on our response.

We believe these elements represent some of the best practices in the industry, and we are continuing to look for ways to improve. For example, one of the key components of our program is system redundancy. We create backup systems to ensure that, if one of our systems is compromised, we can recover operations by turning to a redundant system. We also join other electric providers to strengthen our individual electric systems through the broader network itself. We rely on our neighboring utilities and the regions in which we operate (and, in the same way, they rely on us) to provide backup operations in the event of a significant service disruption.

In addition, under the "Detect" element above, we have joined other utilities to receive information and analysis regarding cyber threats from the E-ISAC – the Electricity Information Sharing and Analysis Center. Managed by the North American Electric Reliability Corporation, or NERC, the E-ISAC serves as the primary security communications channel for the electricity subsector and enhances the subsector's ability to prepare for and respond to cyber threats. While the E-ISAC is an effective and robust information sharing platform, Xcel Energy has recently expanded its information sharing capabilities by joining with the Financial Services ISAC to create a new information sharing community known as the Energy Analytic Security Exchange (or EASE). EASE will take advantage of the state-of-the art capabilities of the FS-ISAC and, together with our membership in the E-ISAC, enhance our ability to identify and respond to threats to the Xcel Energy grid, in particular threats to the SCADA system.

Our collaboration with the FS-ISAC in creating EASE is part of our effort to design a flexible cybersecurity program to meet the evolving nature of the cyber threat. The success of any cybersecurity program, however, depends first on the people who implement it. At Xcel Energy, I have assembled an excellent team of security professionals. I have hired a Chief Security Officer with 30 years of government and industry experience managing cybersecurity threats. He runs a team consisting of 97 employees, most of who are focused on cybersecurity issues. As the cyber threat has increased, the scope of our cybersecurity program has also grown dramatically. Five years ago, Xcel Energy did not have a Chief Security Officer, and its cybersecurity staff was a fraction of what it is today. As with every aspect of our business, we work hard to ensure that our security program is efficient and cost-effective, but make no mistake: cybersecurity is not free, and our customers are paying for the programs we need to protect the grid.[1]

I am proud of our cybersecurity program and the progress that we are making. However, our program is and always will be a work in progress. It is not perfect, and it must continue to grow and change as we learn more about the threat we face.

Technology Advancements Are Enhancing the Defense of the Grid.

Our enemies are constantly deploying new technologies to attack the electric grid, and we must create our own defensive technologies to respond. The good news is that we are beginning to deploy these new technologies to help respond to these threats. Below is a partial list of some of the technological advancements that are helping us to defend our grid:

Information Sharing Tools. As cyberattacks continue to increase in scope, we need better tools to identify the attacks and respond before they can trigger an outage. Information sharing tools must become more sophisticated as attacks become more sophisticated. Fortunately, our arsenal of information sharing tools is continuously improving. The E-ISAC deploys the Cybersecurity Risk Information Sharing Program, or CRISP, to facilitate the exchange of detailed cybersecurity

[1] In order to maintain an effective cyber security program, we are required to invest in expensive, state-of-the-art technologies to keep pace with the constantly evolving threat. The attackers however, can still heavily rely on exploits that are 10-15 years old and are still as effective as when they first came out.

information between the industry, the E-ISAC, DOE, and Pacific Northwest National Laboratory (PNNL). CRISP has potential to be a valuable information sharing tool. Twenty-six utilities in North America leverage CRISP to obtain secure access to information and analysis of cyber threats identified by the nation's intelligence apparatus.

Information sharing will become more effective if it allows machines to communicate directly with each other without human interaction. Low-cost machine-to-machine information sharing tools, including STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Indicator Information) have now become state-of-the-art information sharing technology for the nation. In fact, the experience of the FS-ISAC with these tools was one of the reasons that we created the EASE program under the FS-ISAC. Real time, machine-to-machine information sharing will enhance our ability to respond to grid attacks before they can impact customers.

Operating Technology Improvements. If the SCADA system, which houses the main computer and processing functions, is the like the brain of the utility's central nervous system, the grid and breakers and other field devices are like the branches with which it communicates. These devices actually do the work of operating the grid. The cyber systems that manage and control these devices are known as operating technology, or OT. The OT system can interface with the company network. Unlike the central SCADA system or the company's network IT systems, which are constantly and often automatically updated with service packs, new releases and bug fixes, these OT devices are frequently running the same software they used when initially installed 10 to 15 years ago. Moreover, these devices have virtually no security capabilities because they were installed at a time when a physical separation from the network IT systems was considered to be "secure." Studies show that upwards of 30% of vulnerabilities identified within OT devices have no patches. Nevertheless, there are some technology upgrades that can help enhance OT security. Specifically, upgrades to the monitoring and control capabilities of the OT systems would greatly improve our ability to protect the grid.

For example, as I mentioned previously, APT malware deposited in a network can lie dormant for years until an enemy decides to exploit it. One of the key components of an effective cybersecurity program is the ability to monitor and identify system threats. Today, we are beginning to deploy new "hunt" technology in our network that will look for anomalies and changes on the network that could indicate the presence of malware. Hunt technology will become critical to protecting the system in the future as the pace of cyberattacks increases.

Similarly, improved monitoring capability within the SCADA itself will provide a real-time detection capability of changes to the environment. Some types of malware include features that mask the execution of an attack while it is occurring. With this masking feature, system operators might not be aware that the system is under attack even as the lights turn off across the grid. Improved monitoring technology can help protect against this kind of attack. Because the SCADA environment is static compared to the average IT environment, changes, especially numerous changes in a short period of time, are very suspicious. Improved monitoring designed specifically for the SCADA environment would identify new device connections and communications that may demonstrate the presence of cybercriminal in the system.

Industry and the Government Have Developed a Strong Program to Coordinate a Response to Cyber Threats.

Defense of the grid is the responsibility of every utility company in America. However, given the nature of the threat and the nation-wide interconnectedness of the grid, it is also a national security priority. For that reason, the electric industry and federal national security agencies must work together to establish effective cybersecurity programs. Although, as I will discuss later, there is always more to do, I am pleased to report that the nation's cybersecurity programs are strong, collaborative and continuing to evolve to meet the cybersecurity threat.

<u>Cybersecurity Regulation and Emergency Orders</u>. First, the utility industry is subject to mandatory cybersecurity regulations. Under the Federal Power Act and Federal Energy Regulatory Commission oversight, the electric power sector is subject to NERC Critical Infrastructure Protection (CIP) Reliability Standards that include cyber and physical security requirements. Entities found in violation of CIP standards face penalties that can exceed $1 million per violation per day.

These mandatory standards continue to evolve with input from subject matter experts across the industry and government. Currently, the electric power sector must comply with Version 6 of the cybersecurity standards, and additional modifications are underway to add new requirements mirroring best practices in cybersecurity.

In addition to implementing Version 6 of the cybersecurity requirements, NERC and the industry are developing new requirements to address supply chain cybersecurity. The industry also is implementing new mandatory requirements for physical security as part of the broader suite of NERC regulatory standards.

The industry also uses voluntary standards, such as the NIST Cybersecurity Framework I mentioned previously, as well as DOE's Cybersecurity Capability Maturity Model. Like Xcel Energy, electric companies throughout the industry assess their cybersecurity programs and capabilities against this framework and use their assessments to strengthen cybersecurity.

In addition to these mandatory and voluntary standards, Congress recently took steps to ensure a single government entity would have emergency authority and ultimate responsibility in the event of a true grid security emergency resulting from a cyberattack or other types of intentional or existential threats to the grid. The 2015 transportation bill ("Fixing America's Surface Transportation Act" or FAST Act) provides that, upon a Presidential determination of a grid security emergency, DOE has authority to issue an order for emergency measures to be taken by

NERC, a regional entity, or electric sector owners and operators. The industry commends Congress for your foresight in addressing this issue, and we are working with DOE to determine the scope and process for such emergency orders. We also appreciate language in the bill providing liability protections for actions taken in compliance with an order, as well as important protections against public disclosure of sensitive critical energy infrastructure information shared with DOE and FERC.

While regulations, standards and orders can provide a solid foundation for strengthening the industry's security posture, they alone are insufficient. In fact, without more, the standards can lead companies to focus solely on compliance without adapting to a mutating threat. As the threats evolve, the nation's security efforts must evolve too. For that reason, industry coordinates cybersecurity policy developments with the ESCC.

The ESCC's Strategic Plan. The ESCC in its current form arose as a result of a NIAC recommendation, and NIAC points to the ESCC as a model for how critical infrastructure sectors can more effectively partner with government. In fact, the ESCC has been a catalyst for major initiatives that are improving the security posture of the industry and, by extension, the nation.

The ESCC is comprised of the chief executive officers of 22 electric companies (including Xcel Energy) and nine major industry trade associations. This group—which includes all segments of the industry, representing the full scope of electric generation, transmission, and distribution in the United States and Canada—serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level incidents or threats to critical infrastructure.

A key characteristic of the ESCC is executive engagement. In addition to providing resources and accountability that have pushed both the government and industry to work together very closely, senior executives on both sides also help to ensure unity of effort and unity of message among their organizations. During an incident, the ESCC's role—while not operational—is to provide situational awareness, ensure coordination with government on response and recovery efforts, and align messaging.

The industry and government leaders are focusing on four main areas that improve the security posture of the industry and the nation:

1. Tools & Technology: Deploying government technologies that improve situational awareness and enable machine-to-machine information sharing, such as those technologies discussed previously in my testimony;

2. Information Flow: Making sure actionable intelligence and threat indicators are communicated to the right people at the right time in the right way;

3. Incident Response and Recovery: Planning and exercising to coordinate responses to an incident;

4. Cross-Sector Coordination: Working closely with other interdependent infrastructure sectors (*e.g.*, communications, downstream natural gas, financial services, water) to ensure all are prepared for, and can respond to, national-level incidents. On behalf of the ESCC, I serve as the electric sector's liaison to the financial sector to help coordinate cybersecurity policies and programs between the two sectors.

Cyber Mutual Assistance. The ESCC builds on existing utility and governmental strengths to respond to this new threat. For example, the electric power industry has long had a culture of mutual assistance; when a weather event or natural disaster impacts a region, crews and lineworkers from all over North America descend on the affected region to restore power. As cyber risks proliferate, the industry, with the ESCC's leadership, has moved to develop a cyber mutual assistance program to aid electric companies in restoring necessary computer systems following a regional or national cyber incident. This program builds on the industry's culture of mutual assistance to develop resource-sharing relationships that can provide surge capacity should a cyber incident exceed the capacity for an individual company to respond. Xcel Energy is participating in the cyber mutual assistance program.

Exercises. The ESCC also works with NERC to simulate the effect of a major cyberattack. Electric companies plan and regularly exercise for a variety of emergency situations—including cyberattacks—that could impact their ability to provide electricity. The largest exercise so far, in November 2015, was the third biennial industry-wide grid security and incident response exercise known as GridEx III, which brought together more than 364 organizations and 4,400 participants from industry, government agencies, and partners in Canada and Mexico to participate in a rigorous and comprehensive two-day drill that simulated coordinated cyber and physical attacks on the energy grid. GridEx III was a continuation of industry-government efforts to participate in exercises that strengthen the security and resiliency of the energy grid.

In its GridEx III After-Action Report, NERC found that, since GridEx II in 2013, industry and government responses to a significant cyber/physical attack continued to improve. The report identified a number of recommendations for industry and government to continue to strengthen their coordination, preparation, and response capabilities. As was the case with GridEx I and II, these recommendations provide a road map for how the ESCC and the government should address security issues. GridEx IV is scheduled for November 2017.

Other recent national-level exercises in which the industry has participated include: Clear Path IV, conducted by DOE in April 2016; Cascadia Rising, sponsored by FEMA in 2016; Cyber Guard, a two-week DOD-NSA cyber exercise involving experts from government and the energy, IT, and transportation sectors; and a Treasury Department Joint Financial Services-Electric Sector Cyber Exercise in August 2016 that examined incident response capabilities and interdependencies between the two sectors.

Supplemental Operations Strategies. One example of "lessons learned" from these exercises and the December 2015 cyber incident affecting Ukraine is a renewed focus on supplemental strategies for operating the energy grid under sub-optimal circumstances. As I discussed previously, the automation of the SCADA system can leave the grid more vulnerable to cyberattacks. Whether resorting to manual operations, engaging in planned separations, leveraging secondary and tertiary back-up systems, or operating in other degraded states, the industry is working with grid experts to explore "extraordinary measures" – before the incident occurs – to limit the impact and facilitate system restoration in the event of a loss of the automatic control of the SCADA. At Xcel Energy, we are working in parallel with the ESCC to develop our own supplemental operating strategies.

National Laboratories. In addition to working with the Departments of Energy, Homeland Security and Defense, the ESCC also works closely with the national laboratories on research and development of cybersecurity and physical security programs and technologies. For example, as I discussed previously, PNNL developed the CRISP information sharing program. In 2016, Sandia National Laboratory hosted the ESCC to present an overview of its cyber and physical security research. Oak Ridge National Laboratories has evaluated the industry's spare transformer program. Idaho National Laboratories has researched cyber vulnerabilities in gas-fired electric generating units and, for Xcel Energy in particular, undertook an assessment of our new SCADA system.

Emerging Issues. As our industry changes, the cybersecurity threats that we confront also evolve, and the ESCC and Xcel Energy are working to address them. For example, new distributed energy resources (DER) and behind-the-meter assets offer both promise and risk to the grid. DERs and microgrids can improve the capabilities of the grid to withstand outages caused by cyberattacks to the central grid resources. With the appropriate protections (such as those found in a microgrid on a military base), DERs can protect participating customers and even serve as resources to help bring the grid back on line. However, DERs can create new vulnerabilities; these technologies are not subject to the same reliability mandates and security requirements that electric companies must meet, and we do not have organizational control over most customer controlled DER systems. DERs are often connected to the internet and may provide potential entry points for cybercriminals to access to electric companies' grid control systems. DERs increase access points to the grid, and an increase in access points creates additional risks.

Similarly, the installation of billions of "smart" consumer devices may create additional risk. These devices – televisions, thermostats, computers, even refrigerators – have direct connection to the internet and are proving to be vulnerable. While devices comprising the "Internet of Things" (IoT) typically are not directly connected to energy grid infrastructure in the same way as DER, electric companies still recognize the risks related to cyber attacks that may seek to leverage the IoT in a way that would impact the energy grid and electric reliability.

The industry already has faced instances of distributed denial of service attacks similar to IoT-leveraged incidents in other business sectors last year. However, these attacks have focused on business systems (such as customer service), and electric reliability has not been impacted. Nevertheless, in coordination with ESCC, the E-ISAC and the government share actionable intelligence with the industry, and electric companies routinely examine their internet-facing systems for vulnerabilities to ensure that all systems have adequate protections in place.

Congress and the Administration Should Consider New Approaches to Prepare the Nation for the Growing Cybersecurity Threat.

While the programs that I have described are strong and demonstrate that the nation and the industry are working hard to prepare for the cyber threat, there is more to do. The cyber threat is growing, and our cybersecurity programs must continuously improve to meet the coming challenges. As we say in Minnesota, we have to skate to where the puck is going to be, and we had better skate there quickly.

NIAC Recommendations. In 2016, the National Security Council requested that NIAC prepare a scoping study of the nation's cybersecurity programs and preparedness and make recommendations regarding aspects of cyber risk that should be addressed to greatly improve cybersecurity and resilience of our nation's critical infrastructure, NIAC completed that scoping study earlier this year. A copy of the presentation outlining the recommendations of the scoping study is attached to my testimony as Exhibit A.

The NIAC scoping study points to a fundamental problem with the current national approach to cybersecurity policy: I believe that, despite the progress of the last five years, cybersecurity policy at the federal level is often uncoordinated and unfocused. DOE, DHS, DOD and other federal agencies have overlapping authorities and programs. Within Congress, eleven different committees have jurisdiction over cybersecurity issues. Although the federal laboratories are helping to advance our understanding of cybersecurity technology issues, they are pursuing individual research on multiple cybersecurity issues without the benefit of a clear, common national research agenda. Even within industry, despite some progress in cross-sector collaboration, the different critical infrastructure sectors do not coordinate as well as they should.

As a result, the NIAC scoping study has recommended that the nation adopt a transformative national framework for cybersecurity for critical infrastructure. That framework should seek to focus a single national cybersecurity strategy in the same way that a single agency or company would create a single strategy to protect itself. In other words, the framework would establish a cybersecurity program for "USA Inc." The framework would create a flexible and responsive approach to cybersecurity, evaluate the appropriate cybersecurity structures and authorities, and integrate both public and private sectors to provide an effective national cyber defense. To accomplish this goal, NIAC has developed a recommendation to the President to launch an effort to define the scope of this new framework and identify next steps in implementing NIAC's vision.

Although I am a member of the NIAC, I am not speaking today on behalf of the Council. Nevertheless, I believe that the recommendations of the NIAC scoping study are urgently needed. They would expand on the work already underway and build the successes already achieved to establish a more robust, cross-sectorial approach to cybersecurity. I hope that the President will give these recommendations his full consideration, especially as he continues to develop his cybersecurity executive order.

Cybersecurity Legislation. S. 79, is legislation recently introduced by Senators King, Risch, Heinrich and others regarding cybersecurity and the grid. This bill would establish a pilot program between the energy sector and the national laboratories to look at security vulnerabilities, with a particular emphasis on industrial control systems. This work would be guided in part by a public-private working group made up of relevant federal agencies, the national laboratories and the energy industry. Importantly, the bill is clear that participation in this pilot program on the part of utilities would be purely voluntary. The bill includes liability protections for participants and protects sensitive information from disclosure. The Edison Electric Institute, the association that represents all investor-owned utilities in the nation (including Xcel Energy), does not object to the bill. As my testimony demonstrates, close partnerships with the private sector, such as those envisioned under this bill, would yield benefits to the industry as we work to protect the grid.

Information Sharing. As my testimony makes clear, timely sharing of information is critical to the effectiveness of a cybersecurity program. In that regard, I appreciate this committee's role in enacting the Federal Cybersecurity Information Sharing Act in 2015. That law helped promote information sharing necessary to protect the grid. However, information sharing is only as good as the process by which the government provides information to the private sector. Based on our experience, federal agencies are slow to provide classified information to utilities through the ISACs or other channels. While protection of the nation's secrets is vital, a better process could ensure that we have the necessary information in a timely fashion.[2]

Operations Technology. Finally, as I discussed previously, one of the most significant threats to our industry arises from vulnerabilities to the OT that runs control systems and devices. Research into improved OT safeguards (such as hunt capabilities, monitoring, and encryption) would reduce OT vulnerabilities.

[2] To receive classified information from the government, we must have employees with appropriate security clearances. Unfortunately, the Department of Homeland Security has a significant backlog of pending requests for security clearance. DHS could improve information sharing by reducing this backlog and authorizing appropriate utility employees to receive classified information regarding cyber threats.

FERC is attempting to address these OT vulnerabilities by creating a new CIP standard for the utility sector supply chain. In the utility industry, we are concerned that this new standard would put us in the position of policing the cybersecurity programs for our vendors, which would likely be expensive and unsuccessful. A better approach would be to work with the national laboratories to establish appropriate standards for OT cybersecurity for grid-connected devices, including standards for password protection, communication and other aspects of operations. These standards would become important as we see more and more distributed devices interconnect to the grid.

Thank you again for the opportunity to be with you today. I would be happy to answer any questions.