Executive Summary

Statement of Nadya Bartol
Vice President, Industry Affairs and Cybersecurity Strategist
Utilities Telecom Council
Before the
Subcommittee on Oversight and Subcommittee on Energy
Committee on Science, Space, and Technology
U.S. House of Representatives
September 10, 2015

Founded in 1948, the Utilities Telecom Council (UTC) is a global trade association for the communications and information technology interests of electric, gas and water utilities, pipeline companies and other critical infrastructure industries – both here in the United States and in other parts of the world. The Council serves as the source and resource for our members to deploy technology and solutions that deliver secure, reliable and affordable mission critical services. UTC's mission is to shape the future of utility mission critical technologies by driving innovation, fostering collaboration and influencing public policy.

Summary of the major points of my testimony:

- Cybersecurity cannot be completely solved, and will remain a risk we must actively manage.
- Relying strictly on technical solutions to solve cybersecurity is insufficient and dangerous because people will always circumvent the technology if they are motivated to do so.
- The grid is vulnerable to a variety of threats including individual hackers, activist groups, cyber criminals, and nation states. We can monitor, better understand, and mitigate this threat, but fundamentally it is outside of our span of control.
- Those vulnerabilities that are within our span of control require long-term solutions: shortage of qualified cybersecurity workforce, age of legacy infrastructure, lack of legal framework for information sharing, and evolving practices for assuring security in supplier products and services.

Statement of Nadya Bartol
Vice President, Industry Affairs and Cybersecurity Strategist
Utilities Telecom Council
Before the
Subcommittee on Oversight and Subcommittee on Energy
Committee on Science, Space, and Technology
U.S. House of Representatives
July 30, 2015

Good morning Mr. Chairman and Members of the Subcommittee. My name is Nadya Bartol. I am the Vice President of Industry Affairs and Cybersecurity Strategist at the Utilities Telecom Council. Thank you for the opportunity to testify today about the vulnerabilities of America's power supply.

Background

Cybersecurity presents a serious concern with respect to grid vulnerability. It is a complex challenge that requires comprehensive process-driven solutions. Cybersecurity cannot be completely solved, and will remain a risk we must actively manage as long as society wants to have the conveniences of a modern world increasingly underpinned and enabled by smart interconnected technologies. Technology industry estimates that by 2020 there will be 50 billion interconnected smart devices in the world. Many of those devices will run our electric grid, smart cities, and smart cars. These devices will support and enable improved quality of life we have come to expect from our technology.

Relying strictly on technical solutions to solve cybersecurity is insufficient and dangerous. Today, we can use available technology solutions designed to reduce cybersecurity risks. However, people will inevitably circumvent technology in order to reduce costs, increase efficiencies or just to prove that they can beat the technology. Furthermore, as recent breaches have taught us, lack of understanding and/or training means that even with robust technology solutions our defenses fail us if

people do not understand what the technology is telling them. Whatever the motivation we need to acknowledge and manage the human factor of cybersecurity.

Today's grid is quite resilient. Since the Northeast Blackout in 2003, utilities have implemented reliability standards and smart grid technologies that should substantially reduce the risk of a similar physical world cascade event. These measures will also work to limit the impact of any individual, single point of failure, cyber-related event. Furthermore, the electric industry is working continuously to manage cybersecurity risks and address evolving cybersecurity threats, regulatory requirements, and emerging technologies. Cybersecurity practices in the electric industry are subject to mandatory cybersecurity requirements under the North American Electric Reliability Corporation (NERC) Critical infrastructure Protection (CIP) standards. These standards have improved cybersecurity practices throughout the US energy market. This includes even those companies who are not subject to regulatory jurisdiction, but nonetheless look to these standards for guidance.

In the past, the systems that utilities used to monitor and manage the grid were isolated from the Internet. As utilities have implemented smart grid and other advanced technologies, they have created new and numerous connections across the distribution grid and beyond the utility meter into the home. While these connections should not be direct and can be architected, designed, and operated to minimize risk exposure, the connections' existence by its very nature presents an ongoing risk.

"Security by obscurity" for industrial control systems (ICS) has rapidly disappeared. In addition to the growing interconnection between traditional ICSs and corporate enterprise networks, we have seen a move away from control systems utilizing highly proprietary hardware, software, and protocols. While proprietary protocols are still used , the underlying technology is now largely IT-based, sharing fundamental similarities with traditional IT enterprise network components and more easily

discoverable and understood by the hacker community. Increased use of common IT-based technology exponentially increases the exposure of the electric grid to cyber threat.

Discussion

Some of the variables in the complex cybersecurity grid vulnerability landscape are outside of our span of control. Those can only be mitigated to a certain extent. And while there are a number of variables within our control, there is no easy way to fix them either as mitigating those variables to an acceptable level may take a long time.

With respect to the **vulnerabilities that are outside of our span of control**, the grid is vulnerable to a variety of threats including individual hackers, activist groups, cyber criminals, and nation states. Evidence from several published reports by security researchers, government organizations, and the industry indicates that the threat from nation states has recently increased. I am referring to the Havex and Black Energy malware that has been described in ICS CERT alerts ICS-ALERT-14-176-02A and ICS-ALERT-14-281-01B published in June and December of 2014, respectively. Those two threats specifically target ICSs and related product vendors. Additionally, the Operation Cleaver report that was published by Cylance in December 2014 details activities stemming from Iran that target energy and utility companies throughout the world, including the US and Canada.

With respect to the **vulnerabilities that are within our span of control**, those are related to the shortage of qualified cybersecurity workforce, age of legacy infrastructure, lack of legal framework for information sharing, and evolving practices for assuring security in supplier products and services.

Shortage of qualified and knowledgeable cybersecurity workforce in the energy space. The 2015 Global Information Security Workforce Study, an international survey of nearly 14,000 information security professionals published by ISC^2, estimates the shortfall in the global information security

workforce to reach 1.5 million by 2020. Furthermore, 86 percent of respondents to the ISACA's 2015 Global Cybersecurity Status Report, which surveyed more than 3,400 ISACA members, identified a cybersecurity skills gap. 92 percent of respondents planning to hire more cybersecurity professionals said they expect to have difficulty finding skilled candidates. This problem is exacerbated in the energy space because we have two different sets of systems – systems that run the grid, referred to as Operational Technology (OT) and business or enterprise systems that we refer to as Information Technology (IT). These two sets of systems command a different set of priorities and are served by individuals with different backgrounds, vocabularies, and goals. UTC members have told us that they have tried transplanting an individual from IT to OT and vice versa with somewhat mixed success. We need to educate and train more people, a lot more people, with a skillset blended across IT and OT in order to make a noticeable difference.

This challenge impacts the energy utilities, numerous vendors that supply systems for the grid, including ICSs and communications devices, as well as the integrators who design and integrate larger more complex systems for utilities. Because these systems existed in isolation in the past and were not required to be secure, the ICS manufacturers' use of cybersecurity practices is relatively recent compared to the IT industry as a whole. Techniques commonly used by large IT houses for the last 10-15 years are much newer in the OT space. People need to learn to use them and more people need to apply them to the newly developed systems. This also applies to the myriad of new smart technologies that are currently entering the industrial space that are required for running smart networks and smart cities. The deficit of cybersecurity workforce permeates all levels of the energy utility organization. There are simply not enough cybersecurity journeymen to do the work and not enough cybersecurity leaders to determine what is needed and how to proceed. The same is true for the entire energy utility ICS and information and communication technology (ICT) supply chain.

This is why UTC has partnered with an accredited university to develop a graduate certificate program in Critical Infrastructure Cybersecurity. This program aims to educate IT and OT practitioners, as well as compliance and other technology practitioners in the utility space, in the security aspects of utility systems and networks, holistically addressing both IT and OT.

Legacy Infrastructure. The technology of the grid is in itself a cybersecurity concern. Our grid is based on layers of technology that have accumulated over time. Unlike the high-tech industry that measures generations in terms of the 18-24 month intervals of Moore's Law, grid components measure lifespans in decades. Even the new technology that is now implemented in the grid has not necessarily been designed and implemented with security in mind from the beginning. Bolting on security is proven to be less effective and more expensive than building it in, but the former practice still persists due to perceived higher costs and deficit of knowledgeable workforce. Currently US energy utilities have a variety of legacy equipment that will take years and billions of dollars to replace. This infrastructure was not designed to be secure because security was not a concern when that infrastructure was implemented. Utilities have been utilizing a variety of technologies, methods, and techniques to help manage or mitigate some legacy infrastructure's vulnerabilities. However, this is an ongoing concern. Acquiring and implementing such technologies, modifying network architectures, or replacing legacy infrastructure takes time and resources.

Lack of legal framework for information sharing. The Energy sector suffers from inconsistent threat information throughout the sector. This results in a somewhat fractured response to threats when they arise. Numerous organizations such as DHS ICS CERT and the Energy Sector Information Sharing and Analysis Center (ES-ISAC) are working to improve the quality of threat sharing including how actionable and timely it is. Machine-to-machine methods are offered by DHS and now the ES-ISAC through the Cyber Risk Information Sharing (CRISP) program. But we still need a legal framework for information

sharing that would remove the barriers that remain. UTC is a member of Protecting America's Cyber Networks (PACN) Coalition. We are a strong supporter of the two information sharing bills passed by the House of Representatives in 2015 and are advocating for the passage of Cybersecurity Information Sharing Act (CISA) by the Senate before the end of the year.

Evolving practices for assuring security in supplier products and services. Building robust systems that can be resilient in the face of cybersecurity threats requires considering security from inception. Utilities rely on vendors for system design, development, implementation, and maintenance. To address this challenge, it is critical to discuss the acquirer's security needs and requirements with suppliers, and to articulate those requirements during the procurement process in a productive way. It is also critical to monitor how these requirements are adhered to and to make appropriate modifications throughout the lifecycle of the solution. This is still a challenge in many industry sectors, including the Energy sector. Standards and best practices published over the last 2-3 years provide requirements, methods, and techniques that help address this challenge. This includes NIST Cybersecurity Framework which is broadly used in the Energy space. A number of UTC member organizations established initiatives aiming to address this challenge. This is why UTC recently published a white paper providing a standards-based roadmap for implementing basic cyber supply chain risk management practices. We also have offered numerous workshops and seminars on this topic to our members and to the industry at large. Recently this challenge has been acknowledged by the industry regulator, the Federal Energy Regulatory Commission (FERC). On July 16 FERC requested comments on a NERC proposal to develop a new standard addressing supply chain management.

Conclusion: Cybersecurity is a complex challenge that cannot be solved overnight or permanently. It does not lend itself to a cook book of solutions, nor can we envision every possible scenario to mitigate.

We are dealing with an asymmetric threat. However, there are many actions the industry can take to reduce the cyber-related vulnerabilities of the grid. These actions include:

- Increasing supply of cybersecurity workforce that understands both IT and OT contexts
- Providing incentives to utilities to modify or phase out their legacy infrastructures
- Enacting information sharing legislation that removes current barriers
- Supporting industry-based standardization and NIST Framework implementation to facilitate integration of security considerations into current and future technologies.