Hearing of U.S. House Committee on Energy and Commerce
Subcommittee on Cybersecurity and Emergency Response
DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response

Comments by, Leo Simonovich, VP and Global Head,
Industrial Cyber and Digital Security, Siemens Energy
March 14, 2018

Chairman Upton, Ranking Member Rush, and Members of the Subcommittee:

At a time when the risk of cyberattacks against critical infrastructure is growing exponentially, Siemens applauds the Subcommittee's efforts to better understand all aspects of the topic. In the following comments, I will offer my perspective on the topic as the Global Head for Industrial Cybersecurity and Digital Security at Siemens and share a recent initiative that we are leading with partners in the industrial digital economy.

Siemens and the Growing Cyber-threat to Critical Infrastructure

Siemens is a global technology and manufacturing company that has stood for engineering excellence, innovation, quality, reliability and internationality for nearly 170 years. The company has more than 350,000 employees worldwide in more than 190 countries. In the United States, we employ more than 50,000 people and operate more than 60 manufacturing sites. We supply products and solutions to customers across the entire energy value chain, from oil and gas fields, to the electrical grid, to power generation facilities and transportation infrastructure—along with the software solutions that make it all possible. Siemens has approximately 1,200 cybersecurity experts on staff worldwide, including researchers who continuously challenge the security of our own systems and products before they are sold to customers. Cybersecurity is far from a new topic at Siemens: The first IT Security team at Siemens was established in 1986.

With more than one million devices already connected to our MindSphere Internet-of-Things (IoT) platform, we have first-hand experience with cybersecurity challenges in the age of Industrial IoT. Siemens was the first company to have security integrated in all phases of its industrial product development lifecycle and to be certified by TÜV Süd for this purpose. We also have experience in securing industrial sites by assessing security risks and implementing security measures for our customers based on the IEC62443 standards and Holistic Security Concepts.

Given our deep domain know-how in cybersecurity and the energy sector, Siemens is uniquely positioned to help our customers, governments and society as a whole deal with cyber-threats to critical energy infrastructure. We understand that the stakes have never been higher when it comes to cybersecurity for critical infrastructure—particularly energy systems. In fact, among all industries, energy is the most attacked, and the probability that any energy organization will suffer a cyber-attack is nearly 100%. The number of cyberattacks worldwide continues to grow, with operational technology (OT) becoming a growing target. According to a recent study conducted by the Ponemon Institute, OT cyberattacks now comprise 30 percent of all attacks, with a major impact on productivity, uptime, efficiency and safety. With the rise of cloud, mobile and IoT and now the convergence of IT with OT, critical systems are increasingly

vulnerable to aggressive adversaries and attacks.[1]

This comes at a time when artificial intelligence and big data analytics are revolutionizing the economy, including the energy sector. Billions of devices are being connected by IoT platforms and interacting on a new level and scale. This portends tremendous opportunities for our economy, but with this opportunity comes increased exposure to malicious cyber-attacks.

Fortunately, we also know from the Ponemon study and working with our customers that energy companies recognize that they have a shared concern when it comes to cyber readiness. For example, U.S. oil and gas companies participate in the Oil and Gas Information Sharing and Analysis Center, which collects and synthesizes information and turns it into actionable data about common threats. There is also broad recognition at the corporate board level to address this imperative, reflected in increased cybersecurity spending at these companies. Clearly, there is ample need for collaboration and co-creation to address cybersecurity in the energy sector.

Cybersecurity as an Enabler of the Fourth Industrial Revolution

As the Subcommittee knows, cybersecurity is the basic requirement for protecting critical infrastructure, sensitive data, and maintaining operations in today's world. This means that cybersecurity is more than just a metaphorical safety-belt: It is a critical factor in the success of the digital economy. People, organizations, and even entire societies all over the world need to rely on trustworthy digital technologies. Yet, we cannot expect people to actively support the digital transformation if it cannot be ensured that their data and networked systems are adequately protected according to the current state-of-the-art.

That is why digitalization and cybersecurity are two sides of the same coin and must evolve in parallel. If either one is to work properly, they both have to function seamlessly. That is especially true in an era when digitalization is moving into every area of life. Defects or even outages in the systems that control and network our homes, our hospitals, our factories, our power grids – in fact our entire infrastructure – could have appalling consequences. Modern standards for cybersecurity are an essential prerequisite for people to trust our digitalized world – and it is essential to earn that trust, because digitalization is the linchpin for the future success and prosperity of us all.

This risk can be managed with smart collaboration between industry and government. Our society can and must embrace this digital transformation, or "fourth industrial revolution" as it is often called. People and organizations have to trust digital technologies to be safe and secure; otherwise they cannot accept and embrace the digital transformation. Digitalization and cybersecurity must evolve hand in hand.

To keep pace with continuous advances in the market as well as threats from the criminal world, companies and governments must join forces and take decisive actions. This means making every effort to protect the data and assets of individuals and businesses; preventing damage from people, businesses and infrastructure; and building a reliable basis for trust in a connected and

[1] "The State of Cybersecurity in the Oil and Gas Industry: United States" Sponsored by Siemens and independently conducted by Ponemon Institute LLC.

digital world. Creating a holistic basis of trust can't be achieved by a single company or entity; it must be the result of close collaboration at all levels of society.

A New Charter of Trust for the Digital Economy

Recently, Siemens—along with partners representing some of the largest companies in nearly every sector of the digital economy—committed itself to ten principles to ensure the highest possible level of cybersecurity as this digital transformation unfolds. The partners outlined the key factors we consider essential for establishing a new "charter of trust" between society, governments, business partners and customers. The principles of the charter are listed below. They represent what leaders in the private sector can do to "raise the bar" on cybersecurity across the entire digital economy. As you read the charter, you will notice an overarching theme is a commitment to work collaboratively with governments to address this challenge so that our society can realize the benefits of digitalization. Our company is eager to work with the Subcommittee to share our experience and vision in building greater trust in the digital economy.

<u>Principles for a New Charter of Trust</u>

1. **Ownership for cyber and IT security**: Anchor the responsibility for cybersecurity at the highest governmental and business levels, designating ministries and CISOs; establish clear measures and targets as well as the right mindset throughout organizations –"It is everyone's task".

2. **Responsibility throughout the digital supply chain**: Companies –and if necessary - governments must establish risk-based rules for adequate protection across all IoT layers with clearly defined, mandatory requirements. Ensuring confidentiality, authenticity, integrity and availability by setting baseline standards, such as:

    a. **Identity & access management:** Connected devices must have a secure identity and safeguarding measures that allow only authorized users and devices to use them.

    b. **Encryption:** Connected devices must ensure confidentiality for data storage and transmission purposes, whenever appropriate.

    c. **Continuous protection:** Companies must offer updates, upgrades and patches during a reasonable lifecycle for their products, systems and services via a secure update mechanism.

3. **Security-by-default**: Adopt the highest appropriate level of security and data protection and ensure it is pre-configured into the design of products, functionalities, processes, technologies, operations, architectures and business models.

4. **User-centricity**: Serve as a trusted partner along a reasonable lifecycle –providing products, systems and services as well as guidance based on the customer's cybersecurity needs, impacts and risks.

5. **Innovation and co-creation**: Combine domain know-how and deepen a joint understanding between firms and policymakers on cybersecurity requirements and rules

to continuously innovate and adapt cybersecurity measures to new threats; drive and encourage Public Private Partnerships

6. **Education**: Include dedicated cybersecurity courses in school curriculum, as degree courses in university, professional education and training to lead the transformation of skills and job profiles for the future.
7. **Certification for critical infrastructure and solutions**: Companies –and if necessary - governments must establish mandatory independent third-party certification for critical infrastructure and critical IoT solutions (based on future-proof definitions including e.g. where lives are at risk).
8. **Transparency and response**: Participate in an industrial cybersecurity network to share new insights and exchange early warnings; report incidents beyond today's practice which is focusing on critical infrastructure.
9. **Regulatory framework** : Promote multilateral collaboration in regulation and standardization to set a level playing field matching the global reach of WTO; inclusion of rules for cybersecurity into Free Trade Agreements(FTAs).
10. **Joint initiatives**: Drive joint initiatives including all relevant stakeholders to implement the above principles in the various parts of the digital world without undue delay.

You can learn more about the Charter of Trust at www.charter-of-trust.com. Thank you again for your interest in this topic and willingness to consider Siemens's views.