Statement of Steven C. Conner
President
Siemens Energy, Inc.

United States Senate
Committee on Energy and Natural Resources

An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives

Wednesday, August 5, 2020

Introduction

Chairman Murkowski, Ranking Member Manchin, and Members of the Committee, thank you for the opportunity to testify today. I look forward to sharing the views of Siemens Energy on industry efforts to improve collaboration on various cybersecurity and critical infrastructure protection initiatives with the energy sector.

My name is Steve Conner, President of Siemens Energy, Inc., the U.S. regional entity of Siemens Energy. We have more than 11,000 employees in the United States supporting the country's grid operations at 21 power equipment manufacturing, service and innovation sites. Our headquarters is in Orlando, FL. The United States is our company's largest market worldwide, and Siemens Energy equipment provides secure, resilient technologies that support one-third of America's total daily energy needs.

Siemens Energy has been a reliable partner to the United States government, America's energy producers and its energy providers for decades. We have a deep understanding of the safest and most resilient infrastructure technologies and processes necessary to secure one of our most essential national assets, America's power grid. I appreciate the opportunity to share with you our cybersecurity and supply chain management expertise and how collaboration on these issues, both within our own company and with the public and private sector, is critically important in our efforts to help secure our nation's energy infrastructure.

Siemens Energy Overview

Siemens Energy is the global energy business of the Siemens group, which has been working with its customers on solutions for the evolving demands of industry and society for more than 150 years. With planned stock listing, Siemens' energy business will operate independently as Siemens Energy in the future.

It will offer broad expertise across the entire energy value chain, along with a comprehensive portfolio for utilities, independent power producers, transmission system operators, the oil and gas industry, and other energy-intensive industries. With its products, solutions, systems, and services, Siemens Energy will address the extraction, processing, and transport of oil and gas as well as power and heat generation in central and distributed thermal power plants, and power transmission and technologies for the energy transformation, including storage and sector-coupling solutions. The majority stake in Siemens Gamesa Renewable Energy will round out its future-oriented portfolio. With its commitment to leading the way in decarbonization of the global energy system, Siemens Energy will be a partner of choice for companies, governments, and customers on their path to a more sustainable future. With approximately 90,000 employees worldwide, Siemens Energy will help shape the energy systems of today and tomorrow.

As a highly experienced partner and advisor, we will enable our customers to achieve their ambitious goals and will actively assist them on their way to a more sustainable future – no matter where they are in their journey at the moment. That's because the transformation of the energy sector will be starting out from a wide range of different points and will proceed at different speeds – depending on individual countries' economic development and political agendas, as well as their access to energy sources. Accordingly, we will deploy the entire range of our products, solutions and services to shape this transformation together with our customers and partners. Step by step, but consistently and in the right direction. This requires the courage to accept interim solutions, such as increased efficiency or the use of clean fuels.

In this sense, we see ourselves as the partner of choice for government, business and society. Together, we energize society worldwide, and thus enable successful and sustainable growth. That is our promise and our purpose.

Industrial Cybersecurity and Siemens Energy

Industrial cybersecurity is at the core of Siemens Energy's business. We have pioneered cyber solutions to meet the rapidly evolving needs of the utility industry by enhancing visibility, monitoring, and asset management capabilities across critical and energy infrastructure networks. Our products and solutions have industrial security functions that are built-in by design and turned on by default. They support the secure operation of plants, systems, machines, and networks by our customers.

The energy sector has become a primary target for cyber attacks. In this environment, owners and operators need to be certain that cybersecurity solutions will meet the need for operational technologies (OT). Siemens Energy has worked to develop OT-native cybersecurity for the energy sector with the insights gained from long experience developing equipment and weathering attacks ourselves.

In strengthening their cyber defenses, we navigate our customers through the complex relationship between their information technology (IT) and operational technology (OT) environments. We deliver clarity and focus to help our customers make better decisions. We keep our customers safe with our in-depth market knowledge and comprehensive set of solutions along the full value chain.

Cybersecurity Leadership through Collaboration and Information Sharing

Siemens Energy leverages its experience and expertise by establishing partnerships that advance cybersecurity efforts outside of its own walls in the U.S. and beyond. I would like to share with you some examples of those collaborations with both the public and private sectors.

Charter of Trust. Siemens is a leading contributor in the industry push toward continually advancing cybersecurity. In 2018, at the Munich Security Conference Siemens brought together global organizations to create the Charter of Trust – an initiative to build a foundation for a more secure digital world with a focus on the critical infrastructures essential for national functions. Today, its members have transformed it into a unique initiative of leading global companies and organizations working together to make the digital world more secure. For example, the initiative has been driving this by establishing, piloting and adopting global baseline cybersecurity requirements and concepts.

Energy Cybersecurity Alliance (ECA). Siemens Energy is a founding member of the Energy Cybersecurity Alliance (ECA), a partnership formed to enhance the security and resiliency of the North American energy grid by providing a forum for energy companies and service providers, manufacturers and suppliers of equipment and software to discuss and share potential safety and security-focused solutions.

Siemens ProductCERT. The sharing of information across industry and with the government happens via our ProductCERT team – a dedicated team of seasoned security experts that manages the receipt, investigation, internal coordination, and public reporting of security issues related to Siemens products, solutions, or services. ProductCERT cultivates strong and credible relationships with partners and security researchers around the globe to advance Siemens product security, to enable and support development of industry best practices, and most importantly to help Siemens customers manage security risks.

Cyber Emergency Response Team (CERT) Collaboration. Our product security teams maintain a strong collaboration with the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) run by the Cybersecurity and Infrastructure Security Agency (CISA) in the Department of Homeland Security. This collaboration includes pre-release of our Siemens Security Advisories subject to a non-disclosure agreement. A listing of these advisories disclosing vulnerabilities concerning Siemens products are available dating back to 2011. Siemens has direct contact with 535 teams/CERTs worldwide with 98 of them the United States that also may be notified in advance. This network allows for the globally coordinated release of information to all stakeholders.

ISACs/ISAOs. For applicable products/industry, Siemens Energy participates in select sector-based Information Sharing and Analysis Centers (ISACs) and the Information Sharing and Analysis Organizations (ISAOs) established by the Department of Homeland Security. Siemens Energy maximizes its engagement with ISACs /ISAOs by leveraging experts across our organization. Siemens Energy is constantly looking for additional ways to engage the public sector, including supporting vendor-driven forums that would improve industry involvement and promote wider discussion on vulnerabilities and supply chain risks.

Cybersecurity Partnership with NYPA. And just last week, the New York Power Authority (NYPA) and Siemens Energy announced a new collaboration to develop an industrial cybersecurity Center of Excellence. The partnership is intended to bring the public and private sectors together in order to develop innovative cybersecurity best practices that will serve as a

model for deployment at other utilities. The first-of-its-kind industrial cybersecurity monitoring, research and innovation center will focus on detecting and defending against cyberattacks on critical infrastructure owned and operated by NYPA, the largest state-owned electric utility in the nation.

The announcement is the first step in bringing together a coalition of public sector, private industry and academic partnerships that will build core capabilities needed to identify new and existing cyber threats, adopt new technologies to protect digital infrastructure and close the industry's talent-gap. Successful solutions have the potential to be deployed and commercialized at other public and private organizations that operate critical infrastructure systems in the state of New York and beyond.

Working Together to Secure the Supply Chain

To secure our supply chain Siemens Energy depends on close collaboration and involvement with our customers, partners, suppliers, governments, and standards bodies around the world. I would like to share some of our supply chain security policies and best practices to give the Committee a better understanding of the steps Siemens Energy takes to secure America's energy infrastructure.

Supply Chain Management and Risk Assessment Processes. As part of the Siemens Supply Chain Management (SCM) Standard, all suppliers are evaluated and qualified with respect to a supply chain risk management process. This process aims to safeguard and consistently improve strategic supplier performance by ensuring that the potential of our best and most innovative suppliers is utilized in full. Regular supplier audits are an active part of Siemens' governance of our vendors. Evaluations address technical, commercial, and cybersecurity risks and opportunities.

Binding Cybersecurity Requirements for Suppliers in All New Contracts. We have standard contract language with dedicated sections to address cybersecurity in the supply chain to ensure that related organization, processes, physical and information assets used for design, development, manufacturing and distribution of deliveries conform to applicable standards, such as ISO/IEC 27001, ISA/IEC 62443, ISO 27034, NIST 800-series, NERC CIP or similar.

Secure Access to Data, Product Development and Source Code: Siemens has research, product development, and manufacturing facilities located in multiple countries. These facilities are protected using a defense-in-depth approach that uses both physical and IT-based access controls to protect Siemens assets. We decide where to deploy Siemens technology (e.g. source code, research, manufacturing, etc.) based upon the security level of the organization that will use it. Access to confidential and strictly confidential information is carefully managed, tracked and controlled. Unless required as part of a co-development process with a supplier, Siemens does not share overall product development information with suppliers.

Vulnerability Testing for Components. Our project teams select components from qualified suppliers and review its technical qualifications. The supplier's components are further checked as part of the respective hardware, software, and security testing required by the applicable development process. Pilot builds are carefully reviewed by engineering and initial production units go through a thorough inspection and test process prior to final release. Test results and vulnerability information are aggregated into an approved components database.

Vulnerability Monitoring of Components. We constantly monitor the vulnerability information and potential security issues of the suppliers' components that become part of our products. We use multiple information sources or vulnerability information providers such as the NIST National Vulnerability Database. In the event security issues are identified, corrective action is taken, including disqualification of suppliers. IT Security requirements are cascaded to suppliers through contractual terms.

Asset and Services Classification. Siemens Energy conducts an Asset Classification Process based on the ISO/IEC 27001 standard on information and technology assets and services utilized to develop, manufacture, engineer and/or deliver products and services. The Asset Classification Process defines the security level based on a risk assessment, which results in various methods applied to protect the assets or services at an appropriate level. Additionally, Siemens Energy applies a threat and risk analysis that is based on ISA/IEC 62443 and ISO/IEC 27005 to our product portfolio.

Personnel Risk Assessment. For other products that apply, Siemens Energy complies with the NERC CIP-004-6 standard for personnel risk assessment during the on-boarding process and adheres to customer security policies and procedures prior to accessing assets at customer locations. Siemens performs civil, criminal, and government-sanction background checks for both installation and maintenance personnel where required.

Security During Installation. To secure our products during installation, Siemens Energy provides information regarding the secure configuration of the applicable products and systems within the Operational Guidelines for Industrial Security and by following the recommendations in the product manuals. This provides the capability for the systems integrator and asset owner to support multiple policies and practices as required. Siemens Industrial Security Services can also contribute expertise and support including security consulting, implementation and optimization.

Existing Standards and Established Best Practices. Siemens Energy participates in different standards organizations and has selected as a guiding security standard ISO/IEC 27001 and ISA/IEC 62443 to enhance the protection of our hardware, firmware, and software. We consult with other standards (e.g. IEC 62351, NIST 800 series, NERC CIP, etc.) depending upon the critical infrastructure or vertical market where our products are applied, including IEC 62351 for the energy sector. Where applicable supply chain risk management is recommended to follow the ISO/IEC standards that address supplier risk management, contractual requirements, policies, qualification and monitoring.

Penetration Testing. The independent Siemens Corporate Technology department conducts penetration testing on products that often comprise enterprise systems. This information is provided as a report back to the requesting project manager. Penetration test results requiring follow-up actions are recorded in an issue management system where they are tracked to resolution. Siemens also has an internal audit department with a team for products and solutions testing. They also perform component and penetration testing of enterprise systems.

Vulnerability Detection and Mitigation. Any vulnerability identified by an internal or external party is treated equally according to its criticality. Siemens investigates and reproduces the vulnerability upon receiving the report. Siemens handles the vulnerability in collaboration with the responsible development groups. After the issue is successfully analyzed and handled

and if a patch is necessary to resolve the vulnerability, corresponding updates are developed and prepared for distribution. Siemens will notify the customer directly or publicly release a Siemens Security Advisory with information on the vulnerability and corresponding mitigation measure.

Conclusion

Siemens Energy takes its responsibility to secure our country's critical energy infrastructure very seriously. We do this by collaborating with the public and private sector. I hope the sharing of our current supply chain security and cybersecurity efforts will further strengthen the solid partnerships already in place and create new opportunities to collaborate. We all need to work together to "keep the lights on" in America.

Thank you for the opportunity to present the views of Siemens Energy today. I look forward to answering any questions that you may have.