June 7, 2021

Mr. Michael Coe
Director, Energy Resilience Division
Office of Electricity
U.S. Department of Energy
Mailstop OE–20, Room 8H–033,
1000 Independence Avenue SW
Washington, DC 20585

*Sent via email to: ElectricSystemEO@hq.doe.gov*

**RE: Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure**

Dear Director Coe,

On behalf of our 10,400 employees in the United States at our 84 locations including 26 facilities dedicated to manufacturing, Siemens Energy would like to thank the U.S. Department of Energy for requesting feedback from stakeholders on ensuring the continued security of the United States Critical Electric Infrastructure.

In the U.S., Siemens Energy is headquartered in Orlando, Florida and our strong team of employees is dedicated to serving as a fully integrated, full-service partner and driver of the energy transition. Nearly one quarter of our U.S. workforce works in production operations across our Generation, Industrial Applications, Transmission, and New Energy businesses. Our diversity is our strength, and we are powered by our people and our values. With a focus on sustainability, on the co-creation of innovations with our partners, and on strong engagement in the communities where we operate, we seek not only to deliver on the fundamentals but to lead the energy transformation now.

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. We have 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 critical electric infrastructure.

Siemens Energy appreciates the opportunity to share its cybersecurity and supply chain management expertise. Collaboration on these issues, both within our own company and between the public and private sector, is critically important in the efforts to help secure our nation's critical electric infrastructure.

## Industrial Cybersecurity and Siemens Energy

The severity and frequency of cybersecurity attacks in the energy sector are increasing as cyber criminals, terrorist organizations, and nation state actors become more sophisticated. These threats are moving beyond information technology (IT) and are now directly targeting critical operational technology (OT) assets. Couple this trend with increased investment in digital solutions, and threat actors are presented with an expanding surface area for executing attacks. This leaves many organizations even more vulnerable to cyber threats.

With increasing evidence that relying upon an air-gapped network to assure network security is insufficient protection, owners and operators, along with integrators and suppliers, need to be certain that solutions and products will meet cybersecurity requirements posed by the integration of information and operational technologies (IT-OT). Siemens Energy has worked to develop IT-OT native cybersecurity for the energy sector with the insights gained from long experience developing equipment, and as a solutions provider that integrates the products of other suppliers. Industrial cybersecurity is at the core of Siemens Energy's business.

We have pioneered cybersecurity solutions to meet the rapidly evolving needs of the energy sector by enhancing identification, protection, detection, and response and recovery capabilities across critical electric infrastructure networks. Our products and solutions have industrial cybersecurity 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. Siemens Energy offers an end-to-end suite of cyber defense and intelligence solutions uniquely adapted to the needs of the industrial energy industry and operating technology.

Siemens Energy has and will continue to navigate our customers through the complex relationship between their information technology (IT) and operational technology (OT) environments to strengthen their cyber defenses. 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 energy value chain. This ongoing partnership and constant dialogue with our customers is critical to ensuring the latest technology is deployed to keep America's critical electric infrastructure secure.

## Long-Term Strategy to Secure Critical Electric Infrastructure

The Department rightly identifies strengthening the protection and resilience of America's critical electric infrastructure by examining procurement and supply chain policies as a top priority. Siemens Energy shares that view and is committed to working with partners across government and industry to share information to help secure our critical electric infrastructure.

One of the most effective ways to mitigate risk and reduce threats to the critical electric infrastructure of the United States is to apply a risk-oriented approach based on existing international security standards for the energy community. This approach takes the shared responsibilities of product suppliers, system integrators, and asset owners into consideration and ensures the equipment and services responsible for keeping the lights on are subject to robust yet realistic and plainly articulated supply chain security standards and policies.

Siemens Energy depends on close collaboration and involvement with our customers, partners, suppliers, governments, and standards bodies around the world to secure our supply chain. We are continuously improving a set of global procurement practices that factors in the

advanced persistent threat and continuously growing attack surface that we and our customers face every day.

Our efforts are guided by existing international standards that are sector-specific but also apply across all industries. Leveraging existing standards and best practices and taking a risk-oriented approach to cybersecurity and supply chain regulation, would be the most beneficial way for the Department to best instruct the energy sector on how to secure the U.S. critical electric infrastructure. Any potential of new and overlapping requirements could lead to implementation difficulties and confusion for owners, operators, and vendors.

Industry-driven security standards and proven best practices allow both manufacturers and users of equipment to have a common understanding of how products are securely manufactured and developed and how they should be securely installed and used. A new regulatory regime that deviates from this structure, will likely create a chilling effect on procurement, essential maintenance, service, and operations.

The following are some examples of our policies and best practices that we have implemented to help secure America's critical electric infrastructure:

**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. NIST 800 series, NERC CIP, etc.) depending upon where our products are applied. Where applicable, supply chain risk management is recommended to follow the ISO/IEC 27002:2017, Chapter 15, controls on "supplier relationships" that are considered part of ISO/IEC 27001:2013 implementations. These controls address supplier risk management, contractual requirements, policies, qualification, and monitoring. For suppliers, monitoring and tracking their adherence to security requirements is done through security assessments, combined with specific terms and conditions in our procurement contracts requiring security in the supply chain. We also support the full implementation of NERC CIP-013, Cyber Security - Supply Chain Risk Management. The best practice development effort being led by the North American Transmission Forum, could also inform the Department as it moves forward.

**Supply Chain Management and Risk Assessment Processes.** As part of the Siemens Energy Procurement Principles which must be followed by all employees involved in the procurement process, suppliers are evaluated and qualified with respect to a supply chain risk management process which includes cybersecurity where applicable. 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. Siemens Energy conducts regular supplier audits. These audits are an active part of our governance of strategic vendors. Evaluations address issues such as technical, commercial, and cybersecurity risks and opportunities.

**Secure Access to Data, Product Development and Source Code:** Siemens Energy 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 Energy assets. We decide where to deploy Siemens Energy 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, and even then, under the strict protection of confidentiality agreements, Siemens Energy does not share overall product development information with suppliers.

**Vulnerability Testing for Components**. Our project teams select components from qualified suppliers and review their 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. Any similar testing regime managed by the government should make its best practices available, so manufacturers are empowered to self-verify product security. The "Supply Chain Best Practices" developed by the National Electrical Manufacturers Association (NEMA) would also serve as a valuable resource in this area to the Department.

**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 we identify security issues through our diligent monitoring, Siemens Energy takes corrective action, including disqualification of suppliers if appropriate.

**Asset and Services Classification.** Siemens Energy conducts an Asset Classification Process where applicable 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 when applicable.

**Personnel Risk Assessment**. Siemens Energy adheres to customer security policies and procedures prior to accessing assets at customer locations. IEC 62443 also addresses risks associated with human interaction with industrial control systems. Siemens Energy performs civil, criminal, and government-sanction background checks for both installation and maintenance personnel where required and permitted. It is important to note that the customer site owner has exclusive authority to define access rules and that not all personnel on site, and often very few, are Siemens Energy employees.

**Ensure Adaptation of New Technologies is Secure.** One significant problem in the energy sector is that the lifecycle of the computers controlling the equipment is much shorter than that of the equipment itself. This presents significant challenges to owners and operators for whom control system replacements may be advisable from a cybersecurity perspective, but impractical from a commercial or operational perspective.

Siemens Energy strives to embrace new technologies to keep our customers secure. This includes technologies such as cloud computing, artificial intelligence (AI), blockchain, and machine learning (ML), all of which can enhance the security of critical electric infrastructure. For example, DeepArmor® Industrial Fortified™ by Siemens Energy solution allows our customers to use AI and machine learning to protect those legacy systems, even when operating system and traditional antivirus vendors abandon them. "It's obsolete" is no longer a reason for equipment to be open to cyber attacks.

**Enhancing Resiliency with Digitalization and Reserve Equipment.** In addition to the many best practices described above, Siemens Energy would also encourage the Department to take an even more expansive approach to securing U.S. critical electric infrastructure. This could include investing in a critical spare equipment reserve and quick deployment contingency back-up systems. When these systems are equipped with intelligent and automatic grid power flow management solutions, the impact of any incident can be mitigated.

## Conclusion

Siemens Energy is an energy technology leader, and we take our responsibility to secure our country's critical electric infrastructure very seriously. We leverage industry-driven standards, have robust security practices in place, and maintain a supply chain that is vetted, diligently monitored, and diverse. We encourage the Department to use what is described above as a guide when considering its next steps in how best to secure America's critical electric infrastructure.

Securing the critical electric infrastructure supply chain cannot be done solely by the government. It will require the continued collaboration and consultation with original equipment manufacturers. Siemens Energy looks forward to working together with the Department and the entire Federal government to "keep the lights on" in America.

For more information, please contact Brian Raymond, Head of U.S. Government Affairs at Siemens Energy (brian.raymond@siemens-energy.com).

*Respectfully submitted:*

Siemens Energy, Inc.
4400 N. Alafaya Trail
Orlando, FL 32826