June 7th, 2021

Michael Coe
Director, Energy Resilience Division of the Office of Electricity
U.S. Department of Energy
Mailstop OE-20, Room 8G-042
1000 Independence Avenue SW
Washington, DC 20585
ElectricSystemEO@hq.doe.gov

Dear Director Coe,

We are writing in response to your Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure. Claroty Limited is a leading world-wide provider of industrial cyber security solutions to drive visibility, continuity, and resiliency in the industrial economy. Our solutions are deployed in thousands of locations and facilities, in over 50 countries across all seven continents. We serve hundreds of customers, across many industrial verticals including energy generation, transmission, and distribution. Claroty's Operational Technology (OT) platform has been selected, tested, and validated by the world's leading industrial automation and cybersecurity vendors, elite system integrators, and Managed Security Service Providers. We are the only OT security provider to be certified by the U.S. Department of Homeland Security's Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act, which was created to encourage the development and deployment of counterterrorism technologies.

One of the most fundamental issues preventing many companies from effectively securing their OT environments is a lack of visibility into the assets of their Industrial Control System (ICS) environments. It's impossible to protect what you cannot see:

- Without visibility you cannot find and fix vulnerabilities & exposures
- Without visibility you cannot segment your network to limit impact of a cyber incident
- Without visibility you cannot detect and respond to threats in your network

This is why a deep level of visibility into the inner workings of industrial control networks is an absolute imperative and entry point for cybersecurity but also for reducing the cost of ownership for industrial cybersecurity initiatives. Claroty has spent years developing the capability to provider asset owners and operators visibility into what is going on within companies' ICS networks and knowing when there are intrusions or deviations that represent threats and create security risks.

This experience provides us an important and essential perspective for responding to your RFI and proposing policy changes that can advance U.S. energy security.

We have listed our responses below and are also eager to meet and discuss them in greater detail as well as to discuss other ways by which we can help you in ensuring the safety of U.S. critical infrastructure.

1. What technical assistance would States, Indian Tribes, or units of local government need to enhance their security efforts relative to the electric system?

Claroty's role as a key provider of capabilities to protect Operational Technology (OT) environments has given the company insight into the challenges faced by States, Indian Tribes, and local government, in securing critical electric systems. These include: a complex and increasingly dangerous threat landscape; obsolescent and highly vulnerable OT assets; ongoing demand that limits the ability to update systems to protect against vulnerabilities and exposures; an OT culture that is adverse to change; limited experts in OT cyber security to address threats; and the convergence of IT and OT infrastructures.[1] While, individually, each of these factors create cyber risk to OT environments, combined they create system risk beyond regional and local entities' ability to overcome. To address these challenges, we recommend:

- Federal Funding for State, Tribal and Local OT Cyber Security Programs. The Federal Government should create grant programs and other funding to support the adoption of enhanced cyber security capabilities within the State, Tribal and local government providers of the electric sector. One major reason this community of operators has generally been slow to establish effective OT cybersecurity programs is cost: state, tribal and local governments have limited funding and OT security is generally seen as a new cost by utilities that operate on thin margins. A targeted federal grant for the development of OT cyber security capabilities would allow state, tribal and local governments to support the funding of their electric utilities' development of an OT cyber security program, including the hiring of staff and the acquisition, implementation, and operation of technical safeguards and controls.
- Provide Guidance on the Value of Zero Trust Network Access as a Compensating Control. As the digital footprint of network infrastructures continues to expand, it creates a broad surface area susceptible for cyber security attacks. Following a nation-state sponsored

[1] This has become a major threat vector for attackers due to companies' failure to properly secure converged networks when coupled with the inherent challenges of securing OT assets.

attack against Google[2], the concept of Zero Trust was operationalized at the company to ensure this type of event would not reoccur.[3] Zero Trust shifts security controls from the perimeter to individual users and devices in a "trust nothing, verify everything" model.

The U.S. electric system, like all OT environments, suffers from innate challenges that can neither be remediated quickly enough nor be fully secured given the broad range of attack vectors. Implementing Zero Trust Network Architectures can act as a compensating control to rapidly protect vulnerable OT assets. Unfortunately, currently there is a lack of guidance for the use of Zero Trust technologies. To remediate this, consistent with Section 3 of the President's Executive Order on Improving the Nation's Cybersecurity, the Department of Energy should work with the National Institute of Standards and Technology (NIST) to provide guidance to asset owners and operators on the value, deployment, and migration to Zero Trust architectures in order to support the more rapid deployment of such solutions to protect the electric system.

- Encourage the automated adoption of threat and vulnerability intelligence. Because many OT assets were built based upon the assumption of an air-gap: that there would be limited or no connectivity between the OT and IT environments. As a result, many of these technologies were not designed with security in mind, are infrequently patched, and may be obsolescent to the point that they can no longer be remediated. Regardless of the root cause, these assets – and therefore the critical processes they support - are ready targets for cyber criminals and nation states to exploit.

  To remediate this increasing threat, detection technologies must be deployed to enable state, tribal and local government operators of electricity assets to better manage risk in their environments. Additionally, a key part of an OT monitoring technology's detection capabilities is the ability to leverage the most up to date threat and vulnerability intelligence from providers and government agencies to keep current with emerging cyber risks. A recent Claroty research paper found[4] that the energy sector is one of the most highly impacted sectors by industrial control system (ICS) vulnerabilities, with a 74% increase in ICS vulnerabilities between 2018 and 2020. With so many new vulnerabilities being discovered, it is essential that asset owners and operators maintain the latest intelligence on vulnerability discoveries and advisories released from the ICS-CERT and

[2] Operation Aurora - Wikipedia

[3] BeyondCorp | Run Zero Trust Security Like Google

[4] https://security.claroty.com/biannual-ics-risk-vulnerability-report-2H-2020

asset vendors and adopt monitoring and intelligence technology to protect themselves from future attacks. Electric operators should also connect to third party providers to ensure that they are up to date with the latest intelligence. Failures to do so leave asset operators in a position to manually update systems, which can often be forgotten, or not done at all. Encouraging the adoption of automated adoption threat and vulnerability intelligence by state, tribal and local government managers of electricity assets is especially important to protect the energy sector and should be a priority for the coming year.

To help support this important change, FERC should provide guidance for secure architectures to connect to intelligence providers so that these intelligence feeds can keep cyber security teams apprised of at-risk assets in their environments.

- Dedicated Federal Advisors. The Federal Government should grow a cadre of OT cybersecurity professionals that will work with state, tribal and local government to educate them on the technology, provide tools for supporting utility companies. This cadre will be key to implementation as this will be a new technology that state, tribal and other local regulators will not have significant experience to leverage in the implementation stage.

2. What specific additional actions could be taken by regulators to address the security of critical electric infrastructure and the incorporation of criteria for evaluating foreign ownership, control, and influence into supply chain risk management, and how can the Department of Energy best inform those actions?

In addition to the recommendations provided above regarding technical assistance to States, Indian Tribes, and local governments, we believe that the DOE should consider other measures to help support the security of the electric systems, including criteria for evaluating foreign ownership, control, and influence into supply chain management:

- Adapting and Evolving Standards. As OT cybersecurity is a new technology and cost for an electric utility provider, it will be important to establish standards that encourage the adoption of OT cybersecurity technology, and tools that enable buyers of these technologies to know what meets those standards. Currently, companies seeking to buy OT cybersecurity solutions have little way of knowing if a system is as good as the provider's marketing claims. This creates a significant risk of vendors overselling capabilities and energy sector customers thinking they have better protections than they do have.

To address this problem, DOE should work with the National Labs, NIST, and others to establish standards and a labeling regime to demonstrate whether systems have the capabilities they claim and can provide necessary protections. Vendors could submit their solutions for testing to prove their ability to defend against threats to different types of OT systems. The results of this testing would then be used to create a label that would provide customers with information to differentiate between vendors and provide specific solutions with grades for how well they can monitor and protect individual OT systems. Such a grading and reporting system would also protect potential customers from buying deficient systems.

- Encourage More Effective Cyber Resiliency Through Liability Protections. A further means to encourage the mandating and acquisition of an OT cybersecurity program by an electric company would be to establish enhanced liability protections for organizations that make a good faith effort to enhance their cyber resiliency. By providing liability protections for them, this would encourage the vendor community to meet benchmarks and ensure operators of an electric system that they will be protected if they make purposeful decisions on enhancing governance and cyber resiliency. The SAFETY Act is a good model for it. Under it, utilities and other customers that buy certified counter-terrorism technologies such as Claroty's Continuous Threat Detection tool have liability protections from terrorist attacks. A regime that builds off of or expands the SAFETY Act's liability protections could cover domestic terrorism, state actors, and other threats if a company will submit its technology to a rigorous review like that of the SAFETY Act to show it can provide defined protections. If a technology meets those standards, it would provide liability protections for electric system operators that acquire/use it. These protections would provide an additional incentive and protection for system operators in adopting a technology as well as encourage the adoption of proven technologies that, like Claroty's, submitted themselves for a thorough review.
- Foreign Ownership, Control, and Influence (FOCI) Protections and Supply Chain Risk Management. While safeguards to supply chain risk to electric system operators are warranted, we believe that the U.S. Department of Energy (DOE) should be very purposeful in the implementation of criteria for evaluating whether a company's foreign ownership creates risk for procurement purposes. As a first step, DOE should consider whether the recently established Federal Acquisition Security Council (FASC) would be a suitable body to assess these issues. The FASC, which is tasked with developing uniform criteria for supply chain risk management across agencies and establishing procedures for determining if information and communications technology should be removed from federal systems, or excluded from federal systems, would seem to be an appropriate body for DOE to consult in this effort.

It is also worth knowing that foreign-developed OT systems play an importation role in critical infrastructure protection. This includes France's Schneider Electric, Germany's Siemens, and Japan's Yokogawa as well as other vendors and security solution. A too broad limitation on foreign-owned and manufactured technology would limit US access to these companies' key technologies for both operating the energy sector and protecting the sector's key OT systems. This could also hurt economic relationships with U.S. allies that develop many the OT systems and tools critical infrastructure, and other sectors use. We need to ensure we are not treating allies and adversaries similarly. As the adoption of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) showed, a too strict process that does not sufficiently differentiate between ally and adversary countries could overwhelm the system with too many cases for review, slowing down approvals of systems with a foreign nexus. DOE should operationalize a standards approval approach that focuses on practical steps to enhance security and does not draw hard lines that could inhibit efficient operations. This should include: (1) having a broad lens around U.S. Allies to ensure efficiency and promote economic relationships with our trading partners; (2) having a purposeful set of restrictions or approval process around U.S. adversaries to promote national security interests and ensure effective risk mitigation; and (3) ensuring that any approval process be purposeful for efficiency towards these ends.

Finally, to the extent there are supply chain concerns for foreign vendors we should not treat allies and adversaries alike and should work with allies to strengthen and secure their supply chain, including potentially by joint investments in supply chain security.

3. What actions can the Department take to facilitate responsible and effective procurement practices by the private sector? What are the potential costs and benefits of those actions?

In order to ensure effective procurement practices from the private sector, we believe that the DOE can continue to be supportive of current programs:

- **Continued Support of Cyber Testing for Resilient Industrial Control Systems (CyTRICS) Program**.[5] CyTRICS has demonstrated its ability to operate as an effective and influential program to partner with stakeholders to identify high priority OT components, perform expert testing, share information about vulnerabilities in the digital supply chain, and inform improvements in component design and manufacturing. CyTRICS works with test

[5] Cyber Testing for Resilient Industrial Control Systems (CyTRICS) - INL

facilities and analytic capabilities at four DOE National Laboratories. It also has strategic partnerships with key stakeholders including technology developers, manufacturers, asset owners to help address cyber risks to critical infrastructure. DOE should continue to support and expand it. While this RFI is oriented around the electric system, CyTRICS supports multiple subsectors to include Oil & Gas, and Wind & Renewables. CyTRICS providers a partner that can conduct testing and make recommendations at a scale that individual asset owners never could alone.

- Provide incentives. DOE can greatly increase the acquisition of OT cyber security technologies by supporting and incentivizing adoption via grants and liability protections.

4. Are there particular criteria the Department could issue to inform utility procurement policies, state requirements, or FERC mandatory reliability standards to mitigate foreign ownership, control, and influence risks?

In order to help mitigate FOCI risks, we recommend the following steps:

- Policies and regulations should be narrowly tailored to focus on adversaries. The U.S. should have great concerns about protecting its systems against competitors and adversaries like China, Russia, Iran, North Korea and foreign and domestic terrorist groups. We should develop policies to limit the use of their technology and their access to the grid, much like the United States has done by denying certain telecommunications equipment providers access to the U.S. market. When coupled with an effort to collaborate with allies to develop common standards to protect technologies developed outside the U.S. from their influence, this is a good start to better procurement practices.
- Exempt NATO and Major Non-NATO allies such as Japan and Israel from any policies designed to mitigate FOCI. DOE should also be careful not to draw an overly broad rule that applies a traditional Department of Defense/Defense Counterintelligence and Security Agency (DCSA) review to companies based in or owned by a company based in an allied country. Such a strict rule would limit access to these key technologies for the U.S., especially, as the size of the world market is unlikely to give the U.S. necessary leverage to force companies to move their operations completely to the U.S. or submit to the reviews to which defense contractors submit. Additionally, a new FOCI mitigation process could further overwhelm the review system, making it even harder and more time-consuming for companies to go through the FOCI mitigation process, further limiting our access to their technology and overwhelming an already taxed system.

We should limit companies that need to go through FOCI process for foreign ownership to companies that are neither based in a NATO nor non-NATO major ally. This would allow us greater access to their technology for homeland security.

Thank you very much for the opportunity to highlight some of the cybersecurity issues that Claroty experiences in its work with users of industrial control systems in the United States and around the world. If you would like to discuss any of these comments in more depth, please feel free to email me at grant.g@claroty.com.

Sincerely,

Grant Geyer
Chief Product Officer
Claroty
grant.g@claroty.com