FORESCOUT TECHNOLOGIES, INC. RESPONSE TO U.S. DEPARTMENT OF ENERGY REQUEST FOR INFORMATION (RFI) ON ENSURING THE CONTINUED SECURITY OF THE UNITED STATES CRITICAL ELECTRIC INFRASTRUCTURE

Yejin Jang, Government Affairs Director

FORESCOUT TECHNOLOGIES, INC. 190 TASMAN DR., SAN JOSE, CA 95134

The U.S. Department of Energy (DOE) Request for Information on Ensuring the Continued Security of the United States Critical Electric Infrastructure seeks comment on specific actions regulators can take to strengthen capabilities for supply chain risk management for the nation's electric utilities. Forescout Technologies, Inc. (Forescout) respectfully offers the following comments for consideration.

IT and OT convergence in utility environments must be recognized and considered in the development of recommendations, best practices, or regulations

Today's bulk power system (BPS) equipment commonly includes IP-based components that enable communication between the controllers and information technology (IT) components of a utility's network. Even BPS equipment that does not natively have an IP-based component is likely to be connected to other devices that are networked (e.g., the circuit breaker is not networked but the digital relay, human machine interface, or remote terminal unit that controls it, is). Grid modernization and smart grid capabilities have also spurred the growth in operational technology (OT)[1] deployment[2] and by embracing these technologies, electric utilities have gained efficiencies in the monitoring, control, and reliability of the Grid.[3] Increased connectivity in the U.S. electric grid, of both devices and systems (e.g., IT with OT), has also widened the attack surface. The convergence of IT and OT systems has made it impractical to rely on the (presumed) separation of these systems to prevent compromise of those systems by malware or attackers. As DOE contemplates recommendations, best practices, or regulation to combat dynamic cyber threats the focus is, understandably, on the security of OT/industrial control systems. However, and as recent events have shown, IT systems can also impact OT security and utility operations and must be considered alongside any recommendations specific to OT security.

Any regulatory outcome of the DOE's "100-day sprint" and the RFI must be cognizant of the significant investments that BPS owners/operators have made in securing their systems.

In a memorandum (memo) about the 100-day plan that DOE shared with the electric industry, DOE encouraged the rapid deployment of ICS monitoring technologies and asks Electric Subsector Coordinating Council (ESCC) members to identify technologies and systems that can meet several technical capabilities related to visibility, detection, and response capabilities. However, it fails to define key terms such as "collective-defense capabilities" leaving electric utility owners/operators and the cybersecurity industry that serves this community with an ambiguous understanding of the technical capabilities on which DOE sought feedback. Without clear definitions and more details on the data message formats, how intelligence sharing will work and the design/architecture that DOE seeks to achieve, BPS owners/operators are left guessing as to whether their current cybersecurity investments can meet an undefined technical requirement such as "collective-defense capabilities." Definition and clarity about this term and

[1] Gartner defines operational technology (OT) as "hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events," Gartner Glossary, Operational Technology (OT).
[2] Jeff Meyers, How the Convergence of OT Enables Smart Grid Development, page 13, 2013.
[3] Congressional Research Service, Electric Grid Cybersecurity, page 13, September 4, 2018.

DOE's desired mechanisms for threat sharing would greatly assist electric utility owners and operators better align their current investment to DOE's goal of enhancing visibility, detection, and response.

Lay strong cybersecurity foundations with accurate, real-time asset inventory and monitoring (as the concept is reflected in National Institute of Standards and Technology Special Publication 800-137[4]) that enables effective threat mitigation.

The RFI and the currently rescinded E.O. 13920 speak to the prohibition of certain BPS equipment sourced from foreign adversaries. To exclude certain equipment, there is a presumption of awareness that such equipment exists. Effective removal of prohibited equipment depends on an accurate inventory of existing BPS assets. Without knowing what assets are on the network, electric utilities cannot effectively manage connected assets, nor can they then manage these assets' vulnerabilities. Further, accurate asset inventories enable higher-level cybersecurity functions which in turn enable the defense-in-depth strategy advocated by NERC[5] and FERC.[6] In asset management guidance specific to the energy sector, NIST suggests states that "[h]aving an accurate OT asset inventory is a critical component of an overall cybersecurity strategy…These assets must be monitored and managed to reduce the risk of cyber attacks on ICS-networked environments. Key factors in strengthening OT asset management capabilities are determining which tools can collect asset information."[7]

Taking asset inventory a step further, and recognizing that a point-in-time asset inventory is not as valuable as a continuous asset monitoring, the National Institute of Standards and Technology (NIST) has published guidance[8] for organizations to implement an information security continuous monitoring (ISCM) program which aims to "increase visibility into assets and awareness of vulnerabilities. This further enables data-driven control of the security of an organization's information infrastructure and increases organizational resilience." The ISCM

---

[4] Kelley Dempsey, et al., National Institute of Standards and Technology (NIST), Special Publication 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, September 2011.

[5] Defining "defense-in-depth" as: Defense-in-depth is created when there is an appropriate portfolio of performance, risk-, and competency-based mandatory reliability requirements that complement and reinforce each other. North American Electric Reliability Corporation (NERC), Results Based Standards, accessed September 2, 2020.

[6] Federal Energy Reliability Commission, Notice of Inquiry, Potential Enhancements to the Critical Infrastructure Protection Reliability Standards, paragraph 2, June 24, 2020.

[7] James McCarthy, et al., National Institute of Standards and Technology (NIST), Special Publication 1800-23: Energy Sector Asset Management for Electric Utilities, Oil & Gas Industry, page 1, May 2020.

[8] Kelley Dempsey, et al., National Institute of Standards and Technology (NIST), Special Publication 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, September 2011.

concept is also supported by DOE[9] and the U.S. Army Corp of Engineers (USACE),[10] which have both suggested in comments to FERC that the electric sector adopt the NIST concept of ISCM which would provide real or near-real time visibility into all connected assets.

Segmentation and isolation of vulnerable assets is an effective method to protect against insecure BPS equipment and components.

Continuous awareness of connected assets enables implementation of more advanced cybersecurity defenses like segmentation. Dynamic segmentation can effectively minimize or eliminate the risk of lateral movement within connected systems. This is important because many OT networks were designed in flat network topologies which "do not have defense in depth and raise the impact of a successful attack."[11] As IT and OT networks converge, the presence of flat networks common in industrial environments become even more problematic:

> Many OT networks are designed and configured in a flat and unsegmented configuration to simplify the management of the network. Unfortunately, this flat layout increases risk by assuming all systems are of equal importance, function and criticality. A breach of any single device may expose the entire OT network.[12]

Dynamic asset segmentation, which enforces pre-set policies based on a range of device behaviors or attributes, can limit the impact of potential vulnerabilities that seek to move laterally within networks. Special consideration should be given to technologies that can accomplish segmentation in industrial environments. Segmentation in OT-heavy environments requires the use of technologies that can inspect not only IT protocols but also OT protocols.[13] Further, asset discovery and enforcement mechanisms must be sensitive to operational availability as industrial environments like the BPS cannot bear downtime. General Electric suggests three elements for segmentation in industrial control system (ICS) environments:

- Easy virtual zoning without OT network reengineering: Any requirement to physically move equipment for proper segmentation is not only impractical, but out of the question.

---

[9] In response to FERC's report, *Cybersecurity Incentive Policy White Paper*, DOE encourages incentives to deploy continuous network monitoring: "DOE encourages FERC to include incentives to accelerate the development and deployment of (high fidelity) sensor-based continuous network monitoring cybersecurity capabilities for operating the transmission system (e.g., operational technology) in its framework of incentives. This objective not only aligns with the National Institute of Standards and Technology (NIST) Cybersecurity Framework security controls for automated and continuous monitoring, but will also facilitate the efforts of DOE and industry participants to develop and deploy these capabilities across the energy sector… Deployment of such technologies could increase national security by helping to prevent or minimize adverse impacts to energy infrastructure systems, which is crucial for maintaining a reliable energy system." United State Department of Energy, Reply Comments of the United States Department of Energy, page 1, August 28, 2020.

[10] Noting, in response to FERC's NOI, that "[P]roper controls, such as those contained within…NIST's Information Security Continuous Monitoring requirements could prevent initial outages…" United States Army Corp of Engineers, Comments of United States Army Corp of Engineers, page 6, August 25, 2020.

[11] Andrew Lerner, Network Segmentation, Gartner Blog Network, November 9, 2017.

[12] PwC, Cyber savvy: Securing operational technology assets, page 10, December 2015.

[13] "Though IT firewalls may offer network security and segmentation capabilities, they've been designed to inspect IT protocols, not OT protocols," according to General Electric, Network Segmentation for Industrial Control Environments, page 5, 2017..

Critical devices are bulky and/or remotely located. A solution must instead be able to segment a network virtually or logically, even in instances where equipment resides at different sites.

- Zoning with deep packet inspection of OT assets' communications: To properly filter and inspect network traffic across zones, a solution must understand the communication languages of industrial environments, namely the relevant OT protocols (Modbus, DNP3, OPC, and others). That's step one: protocol recognition. The next step is deep protocol inspection.
- Zone-specific OT security policies: Zones must enforce policy specifically created for a particular OT environment.[14]

Effective network and asset segmentation are enabled by accurate asset inventories achieved through practices like continuous monitoring. Value-added functions such as automatic device classification and visualization of communications patterns can also enhance effective segmentation. BPS owners and operators should be encouraged to adopt known best practices to further security in environments where the absence of insecure products and their components cannot be assured.

[14] General Electric, Network Segmentation for Industrial Control Environments, pages 6-7, 2017.