

**Questions for Mr. Puesh Kumar**  
Acting Principal Deputy Assistant Secretary  
Office of Cybersecurity, Energy Security, and  
Emergency Response Department of Energy  
July 27, 2021, Hearing: “Defending the U.S. Electric Grid  
Against Cyber Threats”

QUESTIONS FROM STEPHEN F. LYNCH

During the hearing, you stated that “we don’t manufacture large power transformers in the United States anymore” but indicated that the Biden Administration and the Department of Energy (DOE) are working to “encourage domestic manufacturing” of these transformers. You further testified that you could provide additional information about the companies, and their respective countries of origin, that manufacture large power transformers (LPTs) used throughout the U.S. electrical grid.<sup>1</sup>

- Q1. For each company that manufactures LPTs used in the U.S. electrical grid, please provide:
- a) The name of the company;
  - b) The company’s country of origin or headquarters location; and
  - c) The number of LPTs produced by the company currently in use within the United States.
- A1. Large Power Transformers (LPTs) with capacity above 100,000 kVA (100 MVA) are a critical component of the bulk power system (BPS). Results from a 2020 report by the U.S. Department of Commerce highlighted that suppliers are dominated by foreign-owned companies. The U.S. market for LPTs is less than 1,000 units per year and imports account for more than 80 percent of consumption. Figure VIII-42 from the U.S. Department of Commerce report shows the import quantities of LPTs by the top 10 countries.

---

<sup>1</sup> Subcommittee on National Security, Committee on Oversight and Reform, *Hearing on Defending the U.S. Electrical Grid Against Cyber Threats* (July 27, 2021) (online at <https://oversight.house.gov/legislation/hearings/defending-the-us-electric-grid-against-cyber-threats>).

**Questions for Mr. Puesh Kumar**  
 Acting Principal Deputy Assistant Secretary  
 Office of Cybersecurity, Energy Security, and  
 Emergency Response Department of Energy  
 July 27, 2021, Hearing: “Defending the U.S. Electric Grid  
 Against Cyber Threats”

**Figure VIII-42. Large Power Transformers (>100,000 KVA)  
 Import Quantities by Top 10 Countries (Units, 2015-2020 YTD Jun)**

Country	2015	2016	2017	2018	2019	2019 YTD (Jun)	2020 YTD (Jun)	SUM*
Mexico	297	151	124	150	202	92	139	1,063
South Korea	100	128	123	73	67	27	25	516
Austria	39	60	89	60	103	57	32	383
Netherlands	49	88	51	61	41	20	23	313
Canada	44	41	44	46	63	38	25	263
China	47	27	22	23	25	18	31	175
Taiwan	10	19	18	24	40	20	6	117
Spain	24	12	8	31	1	1	2	78
Brazil	6	7	16	8	14	7	12	63
Poland	6	8	10	13	16	11	3	56

Source: United States International Trade Commission, U.S. Department of Commerce, Bureau of Industry and Security  
 \*Excludes 2019 YTD (Jun) Data

The United States is not manufacturing LPTs in full. According to the Commerce report there are five domestic LPT manufacturers, which are operating at only 40% of capacity and most rely on imports for key transformer components. Domestic production capacity is not adequate to meet demand, especially for extra high voltage transformers (those with >345 kV voltage rating) used for long distance transmission. According to the U.S Department of Commerce report, the domestic industry is volatile with plant closures, company exits and entrances, and acquisitions affecting production capacity.

The U.S. Department of Commerce’s October 2020 report, “The Effect of Imports of Transformers and Transformer Components on the National Security,” provides additional information, including the names of some of the companies that manufacture LPTs. Further, DOE is examining the supply chains for the energy sector industrial base, including for transformers, in response to President Biden’s Executive Order on America’s Supply Chains and will have current information from this analysis.

In response to a question from Rep. Paul Gosar, you stated that DOE has recently received input from industry partners through a request for information (RFI) process about how the United

**Questions for Mr. Puesh Kumar**  
Acting Principal Deputy Assistant Secretary  
Office of Cybersecurity, Energy Security, and  
Emergency Response Department of Energy  
July 27, 2021, Hearing: “Defending the U.S. Electric Grid  
Against Cyber Threats”

States can better secure electrical equipment sourced from foreign countries. You further testified that once the Department has completed its review, you would report back to the Subcommittee with the Department’s findings<sup>2</sup>.

Q2. When does DOE expect this RFI process and its review to be complete?

A2. On January 20, 2021, President Biden issued an Executive Order (EO) on “Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis,” which suspended EO 13920, “Securing the United States Bulk-Power System,” for 90 days. On April 20, 2021, the Department revoked the December 2020 Prohibition Order to create a stable policy environment before the emergency declaration made by EO 13920 expired on May 1, 2021. Also on April 20, the Department announced a new request for information (RFI), “Ensuring the Continued Security of the United States Critical Electric Infrastructure.” The RFI is part of a larger coordinated effort, including the recent “America’s Supply Chains” EO 14017, to develop a strengthened and effective strategy to address the security of the U.S. energy sector. The comment period closed on June 7, 2021, and the Department continues to review the 102 submitted responses, which will inform future policy actions. All submissions have been posted to the DOE website and can be viewed at <https://www.energy.gov/oe/securing-critical-electric-infrastructure>.

In March 2021, the Government Accountability Office (GAO) found that DOE plans for electrical grid security do not adequately address risks to electrical distribution systems and rest upon the assumption that an attack on distribution systems would be “less significant” than an attack on the bulk power system. In response to a question from Rep. Debbie Wasserman Schultz, you committed that DOE would undertake an up-to-date assessment of the potential scale and impacts of a cyber attack targeting one or more electrical distribution systems<sup>3</sup>.

---

<sup>2</sup> *Id.*

<sup>3</sup> *Id.*

**Questions for Mr. Puesh Kumar**  
Acting Principal Deputy Assistant Secretary  
Office of Cybersecurity, Energy Security, and  
Emergency Response Department of Energy  
July 27, 2021, Hearing: “Defending the U.S. Electric Grid  
Against Cyber Threats”

- Q3. Does DOE have an anticipated timeline for the completion of this assessment?
- A3. DOE expects to begin the assessment in FY 2022 and will provide a timeline for completion after review of the scope and deliverables.

During the hearing, you mentioned several programs that DOE has established to help secure the electrical grid against cyber threats, including the Cybersecurity Risk Information Sharing Program (CRISP) and Cyber Testing for Resilient Industrial Control Systems (CyTRICS).

- Q4a. Has DOE established performance goals for the CRISP and CyTRICS programs?
- A4a. For CRISP, DOE and the Electricity Information Sharing and Analysis Center (E-ISAC) track several performance indicators associated with how well the program is operating, specific to intake, analysis, and external communications. The indicators provide an understanding of the current health of the program and are intended to identify areas of potential improvement. As CRISP evolves, DOE will continue work with industry partners, the E-ISAC, and the interagency on opportunities to further refine indicators and establish additional performance goals for the program.

CyTRICS is a newer program for DOE and moved to initial operating capability in early 2021. In its first nine months of operation, CyTRICS signed testing agreements with five manufacturers and asset owners; completed cyber vulnerability testing on three critical components; and has four additional components under review. DOE is currently working with the National Laboratories to characterize the relative resource requirements for testing, as the components currently under review vary significantly in size and complexity. DOE anticipates having better data available to assess throughput capacity for the program in FY 2022. Additionally, as DOE continues to build out CyTRICS program processes—including component prioritization, coordinated vulnerability disclosure, and vendor mitigation—and complete more testing, DOE is establishing the data sources to support analyzing and sharing outcomes from cyber vulnerability testing.

**Questions for Mr. Puesh Kumar**  
Acting Principal Deputy Assistant Secretary  
Office of Cybersecurity, Energy Security, and  
Emergency Response Department of Energy  
July 27, 2021, Hearing: “Defending the U.S. Electric Grid  
Against Cyber Threats”

Q4b. To what extent are the programs currently meeting these goals?

A4b. For CRISP, performance indicators are currently in line with expectations. 2021 is the first full operational year for CyTRICS; consequently, DOE is working with the National Laboratories on establishing resource-related performance indicators.

**Questions for Mr. Puesh Kumar**  
Acting Principal Deputy Assistant Secretary  
Office of Cybersecurity, Energy Security, and  
Emergency Response Department of Energy  
July 27, 2021, Hearing: “Defending the U.S. Electric Grid  
Against Cyber Threats”

QUESTIONS FROM REPRESENTATIVE PETER WELCH

After our intelligence community issued repeated warnings about the threat of using Huawei equipment, the Federal Communications Commission moved to block Huawei products from being used on our communications network. Congress later prohibited U.S. government communications systems from using Huawei equipment.

Q1a. Does the Department of Energy (DOE) have the same concerns about Huawei equipment (e.g. solar inverters, electric vehicle charging stations, etc.) being used on our electric grid?

A1a. Yes. Communications infrastructure underpins grid operations and is increasingly critical as more grid operations are conducted remotely (a trend accelerated during the global pandemic) and as more renewable energy and distributed energy systems (DERs) are introduced into the grid. DERs, such as residential rooftop solar panels and EV charging stations, are connected to the grid via communications infrastructure and comprise part of the “Internet of Things.” Consequently, cyber threats and vulnerabilities to communications systems are a concern for the energy sector. To that end, CESER is working closely with the Office of Energy Efficiency and Renewable Energy (EERE), other technology program offices, the private sector, and through projects under the Grid Modernization Initiative to ensure that cybersecurity is a core component of distributed energy resources.

Q1b. Is there any ongoing review or rulemaking at DOE regarding the use of Huawei equipment in the energy sector?

A1b. DOE has no rulemaking specifically related to Huawei underway. The federal Power Marketing Administrations, which are part of DOE, are subject to FY 2019 NDAA Section 889, which specifically bans use of equipment manufactured by Huawei and other high-risk PRC entities in federal networks; however, provisions in Section 889 only apply to federal networks and systems. For non-federal systems, the regulatory structure of the energy sector is fragmented among federal, state, and local municipalities, and lacks a national-level analogue to the FCC “universal subscriber fee,” which was employed in the communications sector to subsidize replacement of high-risk equipment. Instead, DOE operates a number of programs to illuminate

**Questions for Mr. Puesh Kumar**  
Acting Principal Deputy Assistant Secretary  
Office of Cybersecurity, Energy Security, and  
Emergency Response Department of Energy  
July 27, 2021, Hearing: “Defending the U.S. Electric Grid  
Against Cyber Threats”

cyber supply chain risk for the energy sector for critical digital subcomponents (including software, firmware, virtual platforms, and data) and thereby improve risk management for all high-risk suppliers, to include Huawei and other entities named in FY 2019 NDAA Section 889 as well as FY 2018 NDAA Section 1643. These programs include Cyber Testing for Resilient Industrial Controls Systems (CyTRICS), initiatives related to hardware and software bills of materials between manufacturers and asset owners, and several projects under the congressionally directed Securing Energy Infrastructure Executive Task Force to develop a Cyber-Informed Engineering (CIE) Framework to guide actions the sector can take towards a “security by design” approach. DOE’s cyber supply programs are voluntary but have significant participation from key operational technology manufacturers and energy sector asset owners.