Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

E.O. 13920 and Bulk-Power System Supply Chain Security

June 5, 2020

On May 1, 2020, President Trump issued Executive Order (E.O.) 13920, titled "Securing the United States Bulk-Power System." The E.O. states that it is protecting "the security, integrity, and reliability of bulk-power system electric equipment used in the United States" from "foreign adversaries" who are creating and exploiting vulnerabilities in the bulk-power system (BPS). In the E.O., the President "declared a national emergency with respect to the threat" to the U.S. bulk-power system, with the goal of limiting the acquisition or use of "equipment designed, developed, manufactured, or supplied by" entities subject to the control of foreign adversaries.

According to the Department of Energy (DOE), E.O. 13920 authorizes the Secretary of Energy to

- establish and publish criteria for recognizing particular equipment and vendors for a pre-qualified vendor list;
- identify any now-prohibited equipment already in use, and develop strategies in working with asset owners to identify, isolate, monitor, and replace this equipment as appropriate; and
- work with other appropriate federal agencies to carry out the authorities and responsibilities outlined in the Executive Order.

The order requires that the Secretary of Energy issue implementing regulations by September 28, 2020.

Bulk-Power System Security

The electric grid relies on a number of electronic devices, switches, and circuit breakers to monitor and regulate the flow of electricity. Together, these pieces of mechanical and automated equipment constitute the grid's industrial control system (ICS) network, managing power plant controls, transmission, and distribution substations. There have been increasing reports about foreign hackers targeting ICS on the U.S. grid. While these intrusions have not been reported as causing significant disruptions, concerns are increasing over the potential of such intrusions to result in damaging cyberattacks. Natural gas pipelines, critical to BPS operation, have also been targeted.

Congressional Research Service
https://crsreports.congress.gov
IN11417

Electric power industry operational technology (OT) and information technology (IT) systems rely on hardware devices and software systems, procured from a variety of manufacturers and vendors. Many systems come from international sources due to competition between providers. Many mechanical systems used in the grid, such as power transformers, also are sourced from international vendors, or incorporate components from such vendors. The security of the design, manufacture, and patch management practices of these devices and systems is a potential vulnerability due to their international sourcing, and a perceived lack of consistent oversight of standards and practices to prevent impaired or compromised functionality. If bad actors were to gain access to such devices (especially during the manufacturing process), software could be covertly inserted in the device and activated to impair or take over its functioning.

FERC Supply Chain Risk Management Requirements

In 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing the North American Electric Reliability Corporation (NERC) to develop a Critical Infrastructure Protection (CIP) reliability standard requiring affected entities (e.g., bulk-power system owners, operators, and users) to develop and implement a plan that includes security controls for supply chain management for ICS hardware, software, and services associated with grid operations. In 2017, NERC submitted a petition for approval of the new Reliability Standard CIP-013-1, addressing supply chain risk management, and proposed revisions to two existing reliability standards.

FERC approved the standards in an October 2018 order, with compliance plans originally required by July 2020. Due to the COVID-19 emergency, FERC has approved a delay in implementation of the reliability standards, until October 2020. The standards would require affected entities to develop and implement security controls for ICS hardware, software, and services associated with BPS operations. FERC said that the new standards respond to supply chain risks, including the insertion of counterfeit or malicious software, unauthorized production, tampering, and theft. However, FERC acknowledged in its 2018 order that more needs to be done, as the new standards do not address Electronic Access Control and Monitoring Systems (EACMS) which include firewalls, authentication servers, security event monitoring systems, intrusion detection systems, and alerting systems. FERC directed NERC to develop modifications to the CIP standards to include EACMS within 24 months of the effective date of the order.

Potential Implications of E.O. 13920

E.O. 13920 does not reference the FERC-NERC supply chain reliability standard, nor does it require the involvement of the electric power industry or its vendors in the establishment of DOE's pre-qualified vendor list. While it may be expected that DOE's processes would involve industry stakeholders in meeting its obligations under the executive order, Congress may consider the implications of having two ongoing processes with potentially divergent goals.

Regulations to be issued by DOE would likely determine the level of inspections that may be required. An event in 2019 may be informative regarding the Administration's concerns prior to the issuance of E.O. 13920. A report in the press said that DOE ordered the transfer of a large power transformer to a national laboratory last year. A Chinese manufacturer made the transformer for the Western Area Power Marketing Administration, a DOE power marketing administration. DOE was reported to be concerned that a software backdoor or other cyber vulnerability in the device could cause a failure of the unit.

On the vendor side, agreements between companies resulting in joint ventures or other alliances are often used to reduce business risks and lower costs, especially when manufacturing high-cost but seldom-ordered components, like large high voltage power transformers. Globalization is a reality in the electric power industry supply chain, with international vendors providing components for products for U.S.

company use, and product lines. International alliances are often formed to address increasing development costs, capture advances in technology, and take advantage of production economies of scale to remain competitive.

As federal agencies and affected entities act to protect the reliability of the nation's electricity, Congress may consider the potential for increased costs to consumers and delays to acquisition of equipment from the development and maintenance of a pre-qualified vendor list, as selection, testing, and qualification occurs in an environment of evolving cybersecurity requirements. Congress may also consider issues with recently acquired equipment already in service that may be viewed as suspect or in violation of the executive order.

Author Information

Richard J. Campbell
Specialist in Energy Policy

Disclaimer