Securing the United States Bulk-Power System from Adversarial Threats

May 2020

America's bulk-power system (BPS) is the backbone of the U.S. electric grid, supporting the critical infrastructure that assures our national defense, essential emergency services, economic vitality, and modern way of life. Adversaries continue to develop ways to compromise the BPS, including undermining the supply chain of required critical components. What occurred in Ukraine in 2015 provides an example of this serious threat – attackers gained access to control centers, manipulated breakers at roughly 30 distribution substations, and disrupted power to approximately 225,000 customers.[i] The perpetrators also used malware to erase files and corrupt master boot records, rendering some of the utilities' systems inoperable.[ii]

The 2019 Worldwide Threat Assessment provides numerous incidents pointing to clear evidence foreign adversaries are developing plans and capabilities to launch disruptive cyber-attacks meant to degrade the United States' critical infrastructure.[iii] In 2018 alone, cyberattacks on supply chains increased by 78%[iv], which is the most likely vector for adversaries targeting the grid.[v] Further, according to the 2020 U.S. Counterintelligence Strategy, the number of threat actors and the tools at their disposal only continues to grow.[vi] To confront this advancing threat, President Trump signed the "Securing the United States Bulk-Power System" Executive Order (EO) on May 1, 2020, authorizing the Secretary of Energy, working closely with other federal departments, agencies and U.S. industry, to take proactive measures to protect the BPS.

The EO calls for DOE to develop and publish rules and regulations prohibiting certain acquisitions, import, transfer, or installation of bulk-power system components where there is a credible threat that could compromise the BPS. DOE, working closely with its federal and industry partners, will develop a mechanism to pre-qualify equipment and vendors for the BPS supply chain.

The BPS is defined as facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof) and electric energy from generation facilities needed to maintain transmission reliability. For the purpose of this EO, BPS includes transmission lines rated at 69,000 volts (69 kV) or more, but does not include facilities used in the local distribution of electric energy. The BPS EO will mitigate major threats strictly affecting the BPS, such as substations, control rooms, or power generating stations, including reactors, capacitors, substation transformers, current coupling capacitors, large generators, backup generators, substation voltage regulators, shunt capacitor equipment, automatic circuit reclosers, instrument transformers, coupling capacity voltage transformers, protective relaying, metering equipment, high-voltage circuit breakers, generation turbines, industrial control systems, distributed control systems, and safety instrumented systems.

Because the threat is dynamic, DOE will also lead the newly created *Task Force on the Federal Energy Infrastructure Procurement Policies Related to National Security*, which includes experts from the Departments of Commerce, Defense, Homeland Security, Interior, and the Directors of National Intelligence and Office of Management and Budget, as well as the heads of other agencies as appropriate. The Task Force will work to dynamically track BPS threats, risk-manage and coordinate related federal procurement, and share information and seek the advice of the Electricity Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council.

For additional information regarding the BPS EO, please email bulkpowersystemEO@hq.doe.gov.

---

[i] Department of Homeland Security Cybersecurity and Infrastructure Agency, *ICS Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure*, last revised Aug. 23, 2018, available at https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01; Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, Mar. 3, 2016, available at https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[ii] Ibid.

[iii] Office of the Director of National Intelligence, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*, p. 5 (Jan. 29, 2019), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

[iv] *2019 Internet Security Threat Report: Executive Summary* (Symantec, Feb. 2019), https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-executive-summary-en.pdf.

[v] Idaho National Laboratory, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*, p. 35, https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf.

[vi] National Counterintelligence and Security Center, National Counterintelligence Strategy of the United States of America 2020-2022 (Jan. 7, 2020),https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf