BRACEWELL

INSIGHTS

Guarding the Grid: DOE Releases 100-Day Cybersecurity Pilot Program

April 21, 2021

By: ***Catherine P. McCarthy*** ***Joshua C. Zive***

The February 2021 hack into Oldsmar, Florida's water treatment system is a frightening ***reminder*** that critical infrastructure systems can be vulnerable to cyberattacks and that cyberattacks can jeopardize health and safety. In this case, the hack may have spurred government action. On Tuesday, the Biden administration ***announced*** a 100-day plan "to advance technologies and systems that will provide cyber visibility, detection, and response capabilities for industrial control of electric utilities."

In a coordinated effort among the Department of Energy ("DOE"), the Cybersecurity and Infrastructure Security Agency ("CISA"), and the electricity industry, the plan lays out four areas of focus for the next 100 days: (1) enhancement of mechanisms for detection, mitigation, and forensic activities; (2) "concrete milestones" for the industry to develop "situational awareness and response capabilities in critical industrial control systems (ICS) and operational technology networks (OT)"; (3) reinforcement of overall cybersecurity in critical infrastructure information technology networks; and (4) voluntary industry participation programs "to deploy technologies to increase visibility of threats in ICS and OT systems."

The plan's success likely hinges on the government's ability to develop sustainable, cooperative relationships with the relevant industries. "Public-private partnership is paramount to the Administration's efforts," said National Security Council ("NSC") Spokesperson Emily Horne in ***response*** to Tuesday's announcement, "because protecting our Nation's critical infrastructure is a shared responsibility of government and the owners and operators of that infrastructure." It appears that similar plans are being developed for additional critical infrastructure industries, including water, the chemical sector, and natural gas.

The previous administration responded to the escalating threat of cyberattacks from foreign adversaries*[1]* in part with ***Executive Order 13920***, which declared a national emergency with regard to electric grid security and gave the Secretary of Energy the authority to prohibit certain transactions involving electric equipment potentially controlled by a foreign adversary. Relying on EO 13920, the DOE issued a ***Prohibition Order*** in December 2020 barring "Critical Defense Facilities" and any supporting facilities from purchasing or installing electricity generation equipment manufactured in China ("December Prohibition Order").

On January 20, 2021, President Biden's DOE ***issued*** a 90-day suspension of EO 13920 and the December Prohibition Order to allow the DOE and the Office of Management and Budget to consider methods of "protect[ing] against high-risk electric equipment transactions by foreign adversaries while providing additional certainty to the utility industry and the public." Tuesday's

announcement from the DOE revoked the December Prohibition Order, effective immediately, but EO 13920 will remain in place until it expires on May 1, 2021.

The DOE has now opted to revoke the December Prohibition Order in an effort to "create a stable policy environment" while the DOE further develops its cybersecurity strategy for the electricity sector. However, utilities are still encouraged to "act in a way that minimizes the risk of installing electric equipment and programmable components that are subject to foreign adversaries' ownership, control, or influence" while the DOE develops further recommendations.

To assist in cybersecurity strategy development, along with the DOE's 100-day plan announcement, the DOE issued a ***Request for Information*** ("RFI") "focused on preventing exploitation and attacks by foreign threats to the U.S. supply chain." Interested parties are encouraged to submit input to the DOE by June 7, 2021 regarding the development of "a long-term strategy that includes technical assistance needs, supply chain risk management, procurement best practices, and risk mitigation criteria" as well as the "depth and breadth of a future prohibition authority." Instructions for submitting comments can be found on the DOE's ***website***.

The DOE is still hammering out many details of the 100-day plan, and some details may never be released to the public – expansions of DOE's Cyber Testing for Resilient Industrial Control Systems program, for example, will be classified to avoid oversharing with foreign intelligence. While the DOE works to develop its 100-day plan, utilities should evaluate cybersecurity infrastructure within their own systems. For example, utilities could make renewed efforts to take inventory of software and hardware used across any systems touching critical infrastructure, and ensure that all technology is secure and up to date. If defense, detection, and prevention systems do not meet the DOE's suggested standards, a utility could consider implementing additional measures or strengthening current systems now.

Additionally, a utility could consider whether and how its organization might participate in an information sharing program. Any thoughts regarding guardrails and disclosure limitations for such a program could be submitted as comments to the RFI. Also, a utility could consider how its current approach to communicating with internal and external stakeholders about cyber issues might impact participation in information sharing.

Bracewell is available to assist clients and others with follow-up questions or any concerns about the DOE's new 100-day plan, the effect of the revoked Prohibition Order and expiring Executive Order, and other cybersecurity considerations. We will be monitoring additional developments from the DOE as well as similar cybersecurity plans for other sectors of critical infrastructure and encourage affected organizations to do the same.

---

[1] The new 100-day plan comes not only in the wake of the Oldsmar water system hack but also just days after the administration ***announced*** sanctions against Russia for its role in the Solar Winds hack.