Congress discusses cybersecurity threats and energy infrastructure security

March 23, 2018

At a House Energy and Commerce Committee hearing on energy infrastructure cybersecurity and emergency response on March 14, Department of Energy (DOE) Under Secretary Mark Menezes explained to committee members the severity and pervasiveness of cybersecurity threats, “When you have your security clearance, you get briefed, and your world view changes.” This hearing is the third hearing in a series concerning DOE modernization efforts dating back to January 2018.

The committee discussed a series of bills introduced earlier this month – H.R. 5174, H.R. 5175, H.R. 5239, and H.R. 5240 – that attempt to harden the nation’s energy infrastructure and protect the electric grid and energy supply chain from cyberattacks. However, potential threats to the nation’s energy security and grid resiliency are more than just virtual. The committee also discussed potential emergency response improvements in the face of physical threats due to natural disasters, such as the aftermath from Hurricane Maria damaging the electric grid and leaving roughly 150,000 residents in Puerto Rico still waiting for power to come back after six months. Under Secretary Menezes stated that the DOE recently announced plans to establish the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to mitigate both physical and virtual energy infrastructure threats. CESER would leverage the DOE’s national laboratories to conduct early-stage research and development (R&D) in order to develop the next generation of control systems to better detect, prevent, and recover from cyberattacks. Furthermore, CESER would coordinate with existing public-private energy partnerships, such as the Cybersecurity Risk Information Sharing Program (CRISP) and the Electricity Information Sharing and Analysis Center (E-ISAC), to better lines of communication and information sharing between grid operators and the DOE, decreasing potential grid downtime and enhancing the grid resiliency.

During the hearing, Under Secretary Menezes repeatedly warned the committee of the pervasiveness of malicious cyberattacks on our energy infrastructure and their threat to national security. The Under Secretary’s warning became even more pertinent when, the next day, suspected Russian government-sponsored actors – whose actions have targeted U.S. government entities and multiple critical infrastructure sectors and are being monitored and analyzed by the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) – hacked into a South Dakota-based energy company, multiple nuclear power plants, and power utilities networks to gather control system data, laying the groundwork for a physical disruption. Responding to a separate cybersecurity violation, the Department of Justice unveiled charges on March 23 against nine state-sponsored Iranian nationals who hacked into the Federal Energy Regulatory Commission (FERC) and other federal agencies sensitive to national security during a five-year campaign starting in 2013.

Sources: Department of Energy, Department of Justice, Foreign Policy, Library of Congress, House Energy and Commerce Committee, NPR, US Computer Emergency Readiness Team, Wired Magazine