Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Critical Infrastructure Policy: Information Sharing and Disclosure Requirements After the Colonial Pipeline Attack

May 24, 2021

The ransomware attack against the Colonial Pipeline Company spurred panic buying and fuel shortages along the Eastern Seaboard. Although the attack did not target pipeline control systems, it forced the temporary suspension of fuel shipments via a major pipeline network, according to a company statement. The Biden Administration announced Executive Order (E.O.) 14028 (the EO), "Improving the Nation's Cybersecurity" on May 12, 2021, framing it as a response to the pipeline incident and other recent cyberattacks. While the EO creates requirements that apply to federal agencies and government contractors, the Administration hopes that these actions will have a secondary effect of improving cybersecurity among critical infrastructure companies.

An official, briefing reporters about E.O. 14028, said, "Anybody doing business with the U.S. government will have to share incidents so that we can use that information to protect Americans more broadly." Asked whether the Administration would support congressional efforts to expand information sharing and incident reporting requirements "to a broader set of private companies, perhaps starting with critical infrastructure, such as Colonial," the official responded, "Absolutely."

Using actions aimed at federal agencies to drive critical infrastructure security and resilience (CISR) departs from the policy framework first instituted in the late 1990s and subsequently expanded. The 1998 Clinton Administration executive action, Presidential Decision Directive-63, "Critical Infrastructure Protection," established a framework for public-private partnerships across several designated critical infrastructure sectors. The directive stated that these partnerships should be "genuine, mutual and cooperative," and that market incentives would be "the first choice for addressing the problem of critical infrastructure protection," with regulation used as a last resort in the case of a "material" market failure affecting the health or safety of Americans.

Successive administrations have built upon this partnership and incentive based approach to private sector information sharing and disclosure activities, even as CISR activities have grown and matured. The 2013 National Infrastructure Protection Plan (NIPP), which provides high-level CISR policy implementation guidance to federal departments and agencies, envisions the growth of public-private partnerships in a

Congressional Research Service
https://crsreports.congress.gov
IN11683

"trusted environment" to "establish and pursue a set of mutual goals and national priorities, and employ common structures and mechanisms that facilitate information sharing and collaborative problem solving."

Protecting Information

The statutory framework for CISR policy established under the Homeland Security Act of 2002 (HSA, P.L. 107-296), as amended, also emphasizes voluntary public-private collaboration as the basis for information sharing and disclosure. Congress has generally sought to both create incentives and reduce disincentives for private sector disclosure of sensitive information to federal agencies, rather than enact regulatory mandates. For example, 6 U.S.C. §673 mandates certain safeguards to protect the confidentiality of critical infrastructure information shared with the Department of Homeland Security (DHS) in good faith. Implemented by the DHS Protected Critical Infrastructure Information (PCII) program, this provision shields such information from disclosure under the Freedom of Information Act, from direct use in civil lawsuits, and from disclosure or use in certain other circumstances. DHS's Cybersecurity and Infrastructure Security Agency (CISA) administers the PCII program.

In practice, availability of information sharing programs has not necessarily led private sector owner-operators to use them. A 2006 Government Accountability Office (GAO) report on the PCII program noted that DHS faced challenges that "impede the private sector's willingness to share sensitive information."

Public comments during a 2016 proceeding to update 6 C.F.R. Part 29, which governs the PCII program, echoed some of these concerns. For example, the Association of American Railroads wrote, "The effectiveness of the PCII program is materially undermined by the industry's lack of confidence that submitted information will be properly protected by officials accorded access at any level of government or that breaches will go effectively unpunished." (6 C.F.R. Part 29 has not yet been updated as of this writing.)

Additionally, private sector entities may be unwilling to share sensitive vulnerability or incident information for other reasons, such as avoiding negative publicity or to protect corporate reputations and share prices (if publicly traded), avoiding regulatory penalties, preserving trade secrets, and hiding vulnerabilities from competitors. These factors often impede private sector participation in protected information programs like PCII—federal assurances of confidentiality notwithstanding. This was apparently the case in the recent ransomware attack.

During a May 11, 2021, Homeland Security and Governmental Affairs Committee hearing, CISA's Acting Director said the Colonial Pipeline Company did not immediately disclose the incident or sensitive technical information about the attack to CISA. He said prompt disclosure might have been useful in informing CISA activities to prevent similar attacks against other targets.

The EO calls for DHS to create a board to review significant cyber incidents affecting critical infrastructure, and empowers the board to receive and review a variety of sensitive information. While the board will convene under the auspices of the existing CISR public-private framework, it is unclear whether it will be successful in receiving and securing sensitive industry information.

Recent Congressional Actions

Recent Congresses have taken different approaches regarding sensitive information disclosure. For example, the America's Water Infrastructure Act of 2018 (P.L. 115-270) amended Safe Drinking Water Act water security provisions to revise vulnerability assessment requirements for certain water systems. As revised, water systems are required to assess the "risks to, and resilience of" their critical infrastructure

and certify completion of the assessment—but not submit the assessment or information contained therein—to the U.S. Environmental Protection Agency. Furthermore, water systems are explicitly exempt from disclosing information contained in the assessments "to any State, regional, or local governmental entity solely by reason of the [certification] requirement.... "

Congress provided administrative subpoena powers to CISA, which the agency had sought for several years. Under the authorities, enacted under the National Defense Authorization Act for Fiscal Year 2021 (P.L. 116-283), CISA may issue administrative subpoenas to internet service providers to provide it with subscriber information if such information is needed to identify at-risk critical infrastructure systems connected to the internet. In such cases, CISA would notify critical infrastructure owners of the relevant security risks.

Author Information

Brian E. Humphreys
Analyst in Science and Technology Policy

Disclaimer