Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

# Colonial Pipeline: The DarkSide Strikes

May 11, 2021

On May 8, 2021, the Colonial Pipeline Company announced that it had halted its pipeline operations due to a ransomware attack, disrupting critical supplies of gasoline and other refined products throughout the East Coast. This attack was similar to an earlier pipeline ransomware attack in 2020, which also resulted in a pipeline shutdown. In 2018, cyberattacks reportedly disrupted the customer communications systems (but not pipeline operations) at four of the nation's largest natural gas pipeline companies. The possibility of lengthy pipeline disruptions was raised in 2019 congressional testimony by then-Director of National Intelligence, who singled out pipelines as critical infrastructure vulnerable to cyberattacks that could cause shutdowns "for days to weeks." The Colonial Pipeline cyberattack has elevated concern in Congress about the security of the nation's energy pipelines and government programs to protect critical infrastructure.

## Ransomware

*Ransomware* is a form of malicious software (malware) that seeks to deny users access to data and information technology (IT) systems by encrypting the files and systems—thus locking out users. Perpetrators usually extort victims for payment, typically in cryptocurrency, to decrypt the system. Recently, such attacks have been coupled with data breaches in which perpetrators also steal data from their ransomware victims. In addition to locking their computer systems, the perpetrators notify victims that they have copies of their data and will release sensitive information unless a ransom is paid, extorting them twice. Colonial Pipeline fell victim to the DarkSide *ransomware-as-a-service* (RaaS) variant. RaaS is a cybercrime model in which one criminal group develops the ransomware and hosts the infrastructure upon which it operates, then leases that capability to another criminal group to conduct an attack.

The Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), and the Federal Bureau of Investigation (FBI) have published guides on addressing ransomware attacks. As a cyberattack, ransomware falls subject to the cyber severity schema prescribed in the National Cyber Incident Response Plan. Unlike SolarWinds, this attack only affected one company, so it did not lead to establishing a Unified Coordination Group under the response plan. Instead, because this incident affects energy supplies, the Department of Energy is leading the federal response with support from other agencies.

**Congressional Research Service**
https://crsreports.congress.gov
IN11667

# The Federal Pipeline Security Program

Pipelines are part of the surface transportation critical infrastructure sector. The Transportation Security Administration (TSA) within the Department of Homeland Security (DHS) administers the federal program for pipeline security. The Aviation and Transportation Security Act of 2001 (P.L. 107-71), which established TSA, authorized the agency "to issue, rescind, and revise such regulations as are necessary" to carry out its functions (§101). The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) directs TSA to promulgate pipeline security regulations and carry out necessary inspection and enforcement if the agency determines that regulations are appropriate (§1557(d)). However, to date, TSA has not issued such regulations, relying instead upon industry compliance with voluntary guidelines for pipeline physical security and cybersecurity. Both TSA and the pipeline industry have long maintained that regulations are unnecessary because pipeline operators have voluntarily implemented security programs. Specifically with respect to cybersecurity threats, TSA has testified that "they are emerging—much faster than the Government's ability to write regulations to address them." A 2018 Government Accountability Office report identified weaknesses in TSA's program, including inadequate staffing, outdated risk assessments, and uncertainty about the content and effectiveness of its security standards.

TSA cooperates with the Department of Transportation's (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA)—the federal regulator of pipeline safety—under the terms of a 2004 memorandum of understanding (MOU) and a 2020 annex to facilitate transportation security collaboration. TSA also works with the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), whose mission is primarily "to enhance the security of U.S. critical energy infrastructure to all hazards [and] mitigate the impacts of disruptive events and risk to the sector overall." TSA also cooperates with the CISA, a standalone agency within DHS, whose mission is to "lead the National effort to understand and manage cyber and physical risk to our critical infrastructure." In 2018, DHS announced the Pipeline Cybersecurity Initiative, "a collaborative, coordinated effort between CISA, [TSA], and other federal and private sector partners" to enhance pipeline cybersecurity. TSA also collaborates with the Office of Energy Infrastructure Security at the Federal Energy Regulatory Commission (FERC)—the agency which regulates the reliability and security of the bulk power electric grid.

# Issues for Congress

Congress has investigated ransomware attacks as a growing cybersecurity issue facing the nation. An April 2021 Institute for Security and Technology task force report offers recommendations for addressing ransomware. Congress may choose to consider questions regarding the role of federal agencies in responding to ransomware broadly, in regulated sectors, and within critical infrastructure; the possibility of regulating cybersecurity measures to address cyber risks; ways to deter nation-states from hosting ransomware infrastructure; and the use of cryptocurrencies as an enabler of ransomware attacks.

With respect to the federal pipeline security program, most debate in recent years has revolved around four principal issues. Some in Congress have suggested that TSA's current pipeline security program may require greater resources to more effectively carry out its mission. Other stakeholders have asserted that security standards in the pipeline sector should be mandatory—as they are in the electric power sector—especially given their growing interdependency. Still others have questioned whether Congress should transfer any of TSA's regulatory authority over pipeline security to another agency, such as the DOE, DOT, or FERC, which they believe could be better positioned to execute it. The quality, specificity, and sharing of information about pipeline cybersecurity threats also has been a source of concern.

## Author Information

Paul W. Parfomak
Specialist in Energy and Infrastructure Policy

Chris Jaikaran
Analyst in Cybersecurity Policy

## Disclaimer