6-Government Accountability Office-Colonial

Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness (infographic)

Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness (infographic)

Posted on May 18, 2021

The recent cybersecurity attack on the Colonial Pipeline Company has led to temporary disruption in the delivery of gasoline and other petroleum products across much of the southeast United States.

In today's WatchBlog post, we look at this attack and the federal government and private-sector response. We here at GAO have been warning of cybersecurity threats to critical infrastructure for many years *[Worry]*, and the need to strengthen the federal role in protecting critical infrastructure, which we reiterated in a report issued in March .

Pipeline Vulnerabilities

More than 2.7 million miles of pipelines transport and distribute oil, natural gas, and other hazardous products throughout the United States. Protecting the nation's pipeline systems is a responsibility shared by both the federal government and private industry—with private sector pipeline operators responsible for implementing security measures for their assets *[Disappointment]*. The figure below shows the U.S. pipeline systems' basic components and vulnerabilities. While potential physical attacks are always a concern, the pipeline systems' vulnerabilities can also include various types of cyberattacks, such as infiltration of company business systems or disruption of the systems that control the pipeline's operations.

Image

The Colonial Pipeline Attack

According to the Colonial Pipeline Company, on May 7, the company learned that it was the victim of a cyberattack. Malicious actors reportedly deployed “ransomware” against the pipeline company’s business systems. Ransomware is a type of malicious software that is used to deny access to information technology (IT) systems or data and hold the systems or data hostage until a ransom is paid. A joint DHS/FBI advisory notice confirmed that DarkSide ransomware was used in the attack. This notice explained that to ensure the safety of the pipeline, the company had proactively disconnected certain systems that monitor and control physical pipeline functions so that they would not be compromised *[Rebuild]*. As of May 12, there were no indications that these operational systems had been breached. However, disconnecting these systems resulted in a temporary halt to all pipeline operations. On May 13, Colonial Pipeline reported that it had restarted its pipeline and that product delivery had resumed to all markets.

What Needs to Be Done?

This attack highlights the urgent need to address long-standing cybersecurity challenges facing the nation *[Worry]*. Because systems and networks used by our nation’s critical infrastructure are often interconnected with other systems and the internet, they may be vulnerable to disruptions, such as what has occurred with Colonial Pipeline.

In December 2018 , we reported on weaknesses in the Transportation Security Administration’s (TSA’s) management of its pipeline security efforts, including that the quantity of TSA’s reviews of corporate and critical facilities security had varied considerably. So far, TSA has fully addressed 7 of our 10 recommendations for improving their oversight of pipeline security. However, 3 recommendations related to pipeline security workforce and risk management have yet to be fully addressed.

Further, in September 2020 , we highlighted the need for the federal government to develop and execute a more comprehensive strategy for national cybersecurity and global cyberspace. Since 2010, GAO has made

more than 3,300 recommendations to agencies aimed at remedying cybersecurity shortcomings. As of December 2020, more than 750 of those recommendations are not yet implemented. GAO will continue to assess and report on critical infrastructure cybersecurity protection.

Want to learn more about this issue? Check out our High Risk List page on Ensuring the Cybersecurity of the Nation , which includes a list of recent reports, and also listen to our podcast with GAO cybersecurity experts Vijay D’Souza and Jennifer Franks.