

Colonial Pipeline

On May 12, 2021, Colonial Pipeline announced that its operation system was back online after a ransomware cyberattack shut it down on May 7. When ransomware is successfully installed, it causes the affected central computer system to stop working. Decrypting software was needed to get the computer system working again. A ransom payment to secure the decrypting software was demanded by the hackers for which Colonial Pipeline paid 5 million dollars in crypto-currency.

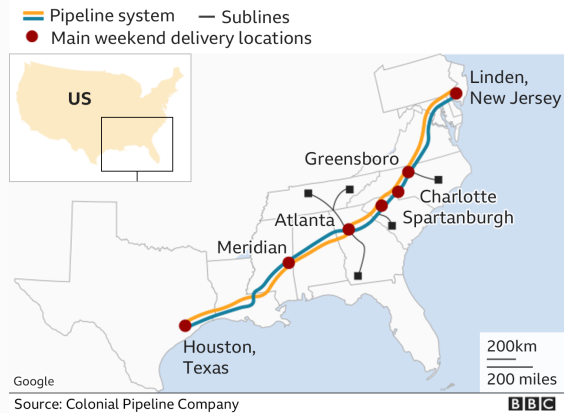
The Colonial Pipeline is the largest gas pipeline in the United States, covering 5,500 miles and providing almost half of the gas supply on the east coast. It is no wonder why the pipeline was targeted by the cyber terrorists. The question is, what does this attack suggest about the United States' preparedness against such attacks and the vulnerability of its technological infrastructure?

So much of how we live is affected by technology. A digital footprint is found in nearly all walks of daily life. From the gasoline pump to the electricity that powers homes and businesses, a central network of computers continually work to scan and check for problems. Despite vigilant efforts, successful attacks on the U.S. technology infrastructure can be catastrophic.




Eighty-five percent of the United States' critical infrastructure is privately owned. There are very few federal regulations mandating whether or how these private companies protect their computer systems. Basically, the federal government leaves it to the private companies to protect themselves from cyberattacks. Once they occur, the National Security Agency collects the data and the Federal Bureau of Investigation investigates the attack, but no federal agency exists to protect these private companies from the attack happening in the first place.

At a recent meeting of the U.S. Senate Homeland Security Committee, Senator Rob Portman (R-OH), was alarmed to learn that there was no specific federal agency charged with securing the federal government's computer systems, let alone an agency responsible for overseeing privately owned critical technology infrastructure.

Colonial Pipeline system map



To Think and To Do: The following bills have been filed in the U.S. Senate. Imagine you are a U.S. Senator. Research each bill. Based on your understanding of each bill and the issues surrounding cyber security, determine whether you would co-sponsor the bill. Explain your reasoning.

Bill Name	Summary	Would you co-sponsor this bill? Yes, No, Unsure	Explain your reasoning.
 S.658 - National Cybersecurity Preparedness Consortium Act of 2021	This bill allows the Department of Homeland Security to work together with a consortium composed of nonprofit entities to develop, update, and deliver cybersecurity training in support of homeland security.		
 S.1324 - Civilian Cyber Security Reserve Act	This bill establishes a Civilian Cyber Security Reserve as a pilot project to address the cyber security needs of the United States with respect to national security, and for other purposes.		
 S.224 - Promoting Digital Privacy Technologies Act	This bill directs the National Science Foundation to support merit-reviewed and competitively awarded research on privacy enhancing technologies.		

Learn MORE about cyber security.

- [What is ethical hacking?](#), from White Hat Security
- [Significant Cyber Incidents](#), from Center for Strategic and International Studies
- [DOD Officials Discuss Cybersecurity at Senate Hearing](#), from Department of Defense

