Major US pipeline struggles to reopen after ransomware attack

May 10 2021, by Virginie Montet

The Colonial Pipeline serves millions of customers on the East Coast, including Washington Dulles International Airport

The US government declared a regional emergency Sunday as the largest fuel pipeline system in the United States remained largely shut down,

two days after a major ransomware attack was detected.

The Colonial Pipeline Company ships gasoline and jet fuel from the Gulf Coast of Texas to the populous East Coast through 5,500 miles (8,850 kilometers) of pipeline, serving 50 million consumers.

The company said it was the victim of a cybersecurity attack involving ransomware—attacks that encrypt computer systems and seek to extract payments from operators.

"This Declaration addresses the emergency conditions creating a need for immediate transportation of gasoline, diesel, jet fuel, and other refined petroleum products and provides necessary relief," the Department of Transportation said in a statement.

The emergency declaration allows for fuel to be transported by road to the affected states: Alabama, Arkansas, District of Columbia, Delaware, Florida, Georgia, Kentucky, Louisiana, Maryland, Mississippi, New Jersey, New York, North Carolina, Pennsylvania, South Carolina, Tennessee, Texas and Virginia.

The declaration also provides regulatory relief to commercial motor vehicle operations that are part of the emergency support efforts.

Colonial said earlier Sunday that it had opened some smaller delivery lines, but the main system was not yet back up and running.

"While our mainlines remain offline, some smaller lateral lines between terminals and delivery points are now operational," Colonial said in a statement, adding it would "bring our full system back online only when we believe it is safe to do so."

"We have remained in contact with law enforcement and other federal

agencies, including the Department of Energy who is leading the Federal Government response," it added.

"Maintaining the operational security of our pipeline, in addition to safely bringing our systems back online, remain our highest priorities."

Calls for improved oversight

Commerce Secretary Gina Raimondo told CBS on Sunday that authorities were working to prevent any disruption to supplies.

Colonial, based in the southern state of Georgia, is the largest pipeline operator in the United States by volume, normally transporting 2.5 million barrels of gasoline, diesel fuel, jet fuel and other refined petroleum products per day.

The attack prompted calls from cybersecurity experts for improved oversight of the industry to prepare for future threats.

"This attack is unusual for the US. But the bottom line is that attacks targeting operational technology—the industrial control systems on the production line or plant floor—are becoming more frequent," Algirde Pipikaite, cyber strategy lead at the World Economic Forum's Centre for Cybersecurity, told AFP on Saturday.

"Unless cybersecurity measures are embedded in a technology's development phase, we are likely to see more frequent attacks on industrial systems like oil and gas pipelines or water treatment plants."

Gas prices jumped in the United States on Sunday following the ransomware attack. Analysts warn that prices could climb even higher if the pipeline is not reopened soon. Oil prices rose more than one percent Monday.

The United States was rocked in recent months by news of two major cybersecurity breaches—the SolarWinds hack that compromised thousands of US government and private sector computer networks and was officially blamed on Russia; and a potentially devastating penetration of Microsoft email servers.

The latter is believed to have affected at least 30,000 US organizations including local governments and was attributed to an aggressive Chinese cyberespionage campaign.