New cybersecurity order issued for US pipeline operators

20 July 2021, by Nomaan Merchant

In this May 11, 2021 file photo, a Colonial Pipeline station is seen in Smyrna, Ga., near Atlanta. The Department of Homeland Security has announced new requirements for U.S. pipeline operators to bolster cybersecurity following a May ransomware attack that disrupted gas delivery across the East Coast.Credit: AP Photo/Mike Stewart

The Department of Homeland Security on Tuesday announced new requirements for U.S. pipeline operators to bolster cybersecurity following a May ransomware attack that disrupted gas delivery across the East Coast.

In a statement, DHS said it would require operators of federally designated critical pipelines to implement "specific mitigation measures" to prevent ransomware attacks and other cyber intrusions. Operators must also implement contingency plans and conduct what the department calls a "cybersecurity architecture design review."

It's the latest response by the Biden administration to a series of ransomware attacks and intrusions hitting critical U.S. infrastructure and raising fears about American cybersecurity.

DHS did not immediately release further details about the guidance, which comes after another directive issued weeks after the May 7 attack on Georgia-based Colonial Pipeline.

U.S. agencies on Tuesday also disclosed that Chinese government-linked intruders targeted 23 natural gas pipeline operators from 2011 to 2013. Thirteen of those attacks were confirmed intrusions, according to a government advisory.

The Colonial attack led to the shutdown of a system delivering about 45% of the gasoline consumed along the East Coast and sparked long lines and gas shortages in several states.

In this May 11, 2021 file photo, a sign marking the location of the Colonial Pipeline is posted in Charlotte, N.C. The Department of Homeland Security has announced new requirements for U.S. pipeline operators to bolster cybersecurity following a May ransomware attack that disrupted gas delivery across the East Coast. Credit: AP Photo/Chris Carlson

Colonial paid an estimated $4.4 million ransom, most of which was recovered by the Justice Department. The FBI has blamed the attack on a

Russia-based gang of hackers using the DarkSide ransomware variant.

The Biden administration has repeatedly accused Russia of granting safe haven to criminal gangs and trying to steal from government agencies and private organizations in various sectors. It imposed sanctions in April for a range of activities including hacking.

Russia has broadly denied being involved in cyberattacks of U.S. institutions, decrying "unfounded accusations" in a statement last month.

The U.S. and key allies this week accused China of complicity in a massive hack of Microsoft Exchange email server software that victimized thousands of organizations. That announcement, however, was not accompanied by sanctions against China, which has accused the U.S. of making "groundless attacks" against it regarding cybersecurity.