10-ZDNet-DHS

DHS releases new mandatory cybersecurity rules for pipelines after Colonial ransomware attack *[Legal Action]*

CISA also sent out an alert saying 13 pipelines had been successfully attacked between 2011 and 2013.

The DHS's Transportation Security Administration (TSA) has unveiled a new security directive forcing owners and operators of important pipelines to put more stringent cybersecurity protections in place. *[Legal Action]*

more coverage

Attack serves as fair warning to persistent corporate inertia over security

This is the organization's second security directive and it applies to all TSA-designated critical pipelines that transport hazardous liquids and natural gas.

The move comes two months after cyber attackers were able to cripple Colonial Pipeline for about a week, leaving millions along the East Coast of the US scrambling for gas.

Colonial had repeatedly postponed a cybersecurity review by the TSA before they were attacked by a ransomware group in May. They ended up paying close to $5 million to the DarkSide ransomware group in order to decrypt their systems. *[Compliance]*

Secretary of Homeland Security Alejandro Mayorkas said the latest security directive would help DHS ensure that "the pipeline sector takes the steps necessary to safeguard their operations from rising cyber threats and better protect our national and economic security."

"The lives and livelihoods of the American people depend on our collective ability to protect our Nation's critical infrastructure from evolving threats,"

Mayorkas said.â€¯“Public-private partnerships are critical to the security of every community across our country and DHS will continue working closely with our private sector partners to support their operations and increase their cybersecurity resilience.”

CISA worked with the TSA on the guidelines and informed the pipeline industry of the cybersecurity threat landscape. They provided technical countermeasures designed to stop the current slate of threats, according to a statement from DHS.

The directive specifically mentions ransomware attacks and lists actions pipelines should take to protect themselves.

It also orders pipeline operators to “develop and implement a cybersecurity contingency and recovery plan, and conduct a cybersecurity architecture design review.”

The first directive was issued in May after the attack on Colonial and orders pipelines to report any confirmed or potential cyberattacks, have a designated cybersecurity coordinator on call 24/7, review security practices and look for security gaps. Pipelines were ordered to do all of this and report the results back to TSA and CISA within 30 days. Those who ignored the orders faced potential fines.

While DHS did not release a detailed list of what was required in the latest security directive, the Washington Post reported that all pipeline operators need to create contingency plans and ways they could recover from an attack. A DHS spokesperson told the newspaper that the directive had “security sensitive information” and would only be distributed to a limited group of people.

Bloomberg News, which first reported that the second security directive was coming, noted that some pipeline operators have balked at some of what is in the directives, including rules that covered password updates, Microsoft macros, and programmable logic controllers.

There has been considerable debate among experts and lawmakers as pressure grows on the government to hold private sector companies

accountable for cybersecurity lapses. Colonial Pipeline and many other pipeline operators ignored cybersecurity reviews by the TSA before the ransomware attack that sparked outrage for weeks. *[Anger]*

In conjunction with the DHS directive, CISA released an alert on Tuesday about a spearphishing and intrusion campaign targeting pipelines that were conducted by state-sponsored Chinese actors from December 2011 to 2013.

Of the 23 attacks on gas pipeline operators discovered by the FBI at the time, 13 were confirmed compromises, three were near misses, and eight had an unknown depth of intrusion, according to CISA.

“CISA and the FBI urge owners and operators of Energy Sector and other critical infrastructure networks to adopt a heightened state of awareness and implement the recommendations listed in the Mitigations section of this advisory, which include implementing network segmentation between IT and industrial control system/operational technology networks,” CISA said in the alert.

“CISA and FBI assess that these intrusions were likely intended to gain strategic access to the ICS networks for future operations rather than for intellectual property theft.”

Security