Official website of the Department of Homeland Security

U.S. Department of
Homeland Security

DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators

Release Date: July 20, 2021

Transportation Security Administration issues second Security Directive

WASHINGTON – Today, in response to the ongoing cybersecurity threat to pipeline systems, DHS's Transportation Security Administration (TSA) announced the issuance of a second Security Directive that requires owners and operators of TSA-designated critical pipelines that transport hazardous liquids and natural gas to implement a number of urgently needed protections against cyber intrusions.

"The lives and livelihoods of the American people depend on our collective ability to protect our Nation's critical infrastructure from evolving threats," said Secretary of Homeland Security Alejandro N. Mayorkas. "Through this Security Directive, DHS can better ensure the pipeline sector takes the steps necessary to safeguard their operations from rising cyber threats, and better protect our national and economic security. 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."

The Department's Cybersecurity and Infrastructure Security Agency (CISA) advised TSA on cybersecurity threats to the pipeline industry, as well as technical countermeasures to prevent those threats, during the development of this second Security Directive. This Security Directive requires owners and operators of TSA-designated critical pipelines to implement specific mitigation measures to protect against ransomware attacks and other known threats to information technology and operational technology systems, develop and implement a cybersecurity contingency and recovery plan, and conduct a cybersecurity architecture design review.

This is the second Security Directive that TSA has issued to the pipeline sector this year, building upon an initial Security Directive (/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators) that TSA issued in May 2021 following the ransomware attack on a major petroleum pipeline. The May 2021 Security Directive requires critical pipeline owners and operators to (1) report confirmed and potential cybersecurity incidents to CISA; (2) designate a Cybersecurity Coordinator to be available 24 hours a day, seven days a week; (3) review current practices; and, (4) identify any gaps and related remediation measures to address cyber-related risks and report the results to TSA and CISA within 30 days.

Since 2001, TSA has worked closely with pipeline owners and operators, as well as its partners across the federal government, to enhance the physical security preparedness of U.S. hazardous liquid and natural gas pipeline systems. TSA works closely with CISA, the nation's lead agency for protecting critical infrastructure against cybersecurity threats, to execute this mission.

Topics: Critical Infrastructure Security (/topics/critical-infrastructure-security) , Cybersecurity (/topics/cyber-security)

Keywords: Cybersecurity (/keywords/cybersecurity) , Pipeline (/keywords/pipeline) , Secretary Alejandro Mayorkas (/keywords/secretary-alejandro-mayorkas) , Transportation Security Administration (TSA) (/keywords/tsa)

Last Published Date: July 20, 2021