U.S. Department of
Homeland Security

DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators

Release Date: May 27, 2021

Today, the Department of Homeland Security's Transportation Security Administration (TSA) announced a Security Directive that will enable the Department to better identify, protect against, and respond to threats to critical companies in the pipeline sector.

"The cybersecurity landscape is constantly evolving and we must adapt to address new and emerging threats," said Secretary of Homeland Security Alejandro N. Mayorkas. "The recent ransomware attack on a major petroleum pipeline demonstrates that the cybersecurity of pipeline systems is critical to our homeland security. DHS will continue to work closely with our private sector partners to support their operations and increase the resilience of our nation's critical infrastructure."

The Security Directive will require critical pipeline owners and operators to report confirmed and potential cybersecurity incidents to the DHS Cybersecurity and Infrastructure Security Agency (CISA) and to designate a Cybersecurity Coordinator, to be available 24 hours a day, seven days a week. It will also require critical pipeline owners and operators to review their current practices as well as to identify any gaps and related remediation measures to address cyber-related risks and report the results to TSA and CISA within 30 days.

TSA is also considering follow-on mandatory measures that will further support the pipeline industry in enhancing its cybersecurity and that strengthen the public-private partnership so critical to the cybersecurity of our homeland.

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. As the nation's lead agency for protecting critical infrastructure against cybersecurity threats, CISA provides cybersecurity resources (https://www.cisa.gov/cyber-resource-hub) to mitigate potential risks, including through a dedicated hub that disseminates information to organizations, communities, and individuals about how to better protect against ransomware (https://www.cisa.gov/ransomware) attacks.

This new TSA Security Directive also highlights the critical role that CISA plays as the country's national cyber defense center. Last December, Congress, through the National Defense Authorization Act,

empowered CISA to execute its mission to secure federal civilian government networks and our nation's critical infrastructure from physical and cyber threats.

Topics: Critical Infrastructure Security (/topics/critical-infrastructure-security), Cybersecurity (/topics/cyber-security), Resilience (/topics/resilience), Secretary of Homeland Security (/topics/secretary-homeland-security)

Keywords: Critical Infrastructure (/keywords/critical-infrastructure), Cybersecurity (/keywords/cybersecurity), Cybersecurity and Infrastructure Security Agency (CISA) (/keywords/cybersecurity-and-infrastructure-security-agency-cisa), Pipeline (/keywords/pipeline), Resilience (/keywords/resilience), Secretary Alejandro Mayorkas (/keywords/secretary-alejandro-mayorkas), Surface Transportation Security (/ntc/surface-transportation-security), Transportation Security Administration (TSA) (/keywords/tsa)

Last Published Date: May 27, 2021