TSA updates, renews cybersecurity requirements for pipeline owners, operators

National Press Release
Wednesday, July 26, 2023

WASHINGTON – The Transportation Security Administration (TSA) announced an update to its Security Directive regarding oil and natural gas pipeline cybersecurity. This revised directive will continue the effort to reinforce cybersecurity preparedness and resilience for the nation's critical pipelines.

Developed with input from industry stakeholders and federal partners, including the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Transportation, the reissued security directive for critical pipeline companies follows the initial directive announced in July 2021 and renewed in July 2022. The directive includes updates that seek to strengthen the industry's defenses against cyberattacks.

"TSA is committed to keeping the nation's transportation systems secure in this challenging cyber threat environment. This revised security directive sustains the strong cybersecurity measures already in place for the oil and natural gas pipeline industry," said TSA Administrator David Pekoske. "Earlier versions required the development of processes and cybersecurity implementation plans. This version requires that operators test and evaluate those plans. We will continue to work with our partners in the transportation sector to increase cybersecurity resilience throughout the transportation system and acknowledge the significant work over the past year to protect critical infrastructure."

Following a May 2021 ransomware attack that disrupted the supply chain, TSA issued security directives mandating that critical pipeline owners and operators implement urgently needed cybersecurity measures in light of the significant cyber threat facing the industry. Since that attack, the threat continues to evolve and intensify. With these revisions to the security directives, TSA continues to take steps to reduce risks to pipeline infrastructure through collaboration with the agency's public and private sector partners.

This security directive requires that TSA-specified owners and operators of pipeline systems take necessary action to prevent the disruption and degradation to their infrastructure. Updates to the security directive require oil and natural gas pipeline owners/operators to:

- Annually submit an updated Cybersecurity Assessment Plan to TSA for review and approval.
- Annually report the results from previous year assessments, with a schedule for assessing and auditing specific cybersecurity measures for effectiveness. TSA requires 100% of an owner/ operator's security measures be assessed every three years.
- Test at least two Cybersecurity Incident Response Plan (CIRP) objectives and include individuals serving in positions identified in the CIRP in their required annual exercises.

Remaining in place are previously established requirements to report significant cybersecurity incidents to CISA, identify a cybersecurity point of contact, and conduct a cybersecurity vulnerability assessment (Security Directive Pipeline 2021-01C).

To view TSA's security directives and guidance documents, please visit: the TSA Cybersecurity Toolkit.