Contact Public Affairs
TSAmedia@tsa.dhs.gov

PRESS RELEASE

FOR IMMEDIATE RELEASE **July 21, 2022**

TSA revises and reissues cybersecurity requirements for pipeline owners and operators

Agency revised cybersecurity requirements to focus on performance-based, rather than prescriptive measures

Revised directive enhances security and resilience

WASHINGTON – The Transportation Security Administration (TSA) announced the revision and reissuance of its Security Directive regarding oil and natural gas pipeline cybersecurity. This revised directive will continue the effort to build cybersecurity resiliency for the nation's critical pipelines.

Developed with extensive input from industry stakeholders and federal partners, including the Department's Cybersecurity and Infrastructure Security Agency, the reissued security directive for critical pipeline companies follows the directive announced in July 2021. The directive extends cybersecurity requirements for another year, and focuses on performance-based – rather than prescriptive – measures to achieve critical cybersecurity outcomes.

"TSA is committed to keeping the nation's transportation systems safe from cyberattacks. This revised security directive follows significant collaboration between TSA and the oil and natural gas pipeline industry. The directive establishes a new model that accommodates variance in systems and operations to meet our security requirements," said TSA Administrator David Pekoske. "We recognize that every company is different, and we have developed an approach that accommodates that fact, supported by continuous monitoring and auditing to assess achievement of the needed cybersecurity outcomes. We will continue working with our partners in the transportation sector to increase cybersecurity resilience throughout the system and acknowledge the significant work over the past year to protect this critical infrastructure."

Following the May 2021 ransomware attack on a major pipeline, TSA issued several security directives mandating that critical pipeline owners and operators implement several urgently needed cybersecurity measures. In the fourteen months since this attack, the threat posed to this sector has evolved and intensified and reducing the national security risk requires significant public and private collaboration.

Through this revised and reissued security directive, TSA continues to take steps that protect transportation infrastructure from evolving cybersecurity threats. TSA also intends to begin the formal

rulemaking process, which will provide the opportunity for the submission and consideration of public comments.

The reissued security directive takes an innovative, performance-based approach to enhancing security, allowing industry to leverage new technologies and be more adaptive to changing environments. The security directive requires that TSA-specified owners and operators of pipeline and liquefied natural gas facilities take action to prevent disruption and degradation to their infrastructure to achieve the following security outcomes:

1. Develop network segmentation policies and controls to ensure that the Operational Technology system can continue to safely operate in the event that an Information Technology system has been compromised and vice versa;

2. Create access control measures to secure and prevent unauthorized access to critical cyber systems;

3. Build continuous monitoring and detection policies and procedures to detect cybersecurity threats and correct anomalies that affect critical cyber system operations; and

4. Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers and firmware on critical cyber systems in a timely manner using a risk-based methodology.

Pipeline owners and operators are required to:

1. Establish and execute a TSA-approved Cybersecurity Implementation Plan that describes the specific cybersecurity measures the pipeline owners and operators are utilizing to achieve the security outcomes set forth in the security directive.

2. Develop and maintain a Cybersecurity Incident Response Plan that includes measures the pipeline owners and operators will take in the event of operational disruption or significant business degradation caused by a cybersecurity incident.

3. Establish a Cybersecurity Assessment Program to proactively test and regularly audit the effectiveness of cybersecurity measures and identify and resolve vulnerabilities within devices, networks, and systems.

These requirements are in addition to the previously established requirement to report signficiant cybersecurity incidents to CISA, establish a cybersecurity point of contact and conduct an annual cybersecurity vulnerability assessment.

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

###

The Transportation Security Administration was created to strengthen the security of the nation's transportation systems and ensure the freedom of movement for people and commerce. TSA uses an intelligence-based approach and works closely with transportation, law enforcement and intelligence

communities to set the standard for excellence in transportation security. For more information about TSA, please visit our website at tsa.gov.