Contact Public Affairs
TSAmedia@tsa.dhs.gov

PRESS RELEASE

FOR IMMEDIATE RELEASE **March 7, 2023**

TSA issues new cybersecurity requirements for airport and aircraft operators

Requirements enhance cybersecurity resilience by focusing on performance-based measures.

WASHINGTON – Today, the Transportation Security Administration (TSA) issued a new cybersecurity amendment on an emergency basis to the security programs of certain TSA-regulated airport and aircraft operators, following similar measures announced in October 2022 for passenger and freight railroad carriers. This is part of the Department of Homeland Security's efforts to increase the cybersecurity resilience of U.S. critical infrastructure and follows extensive collaboration with aviation partners.

"Protecting our nation's transportation system is our highest priority and TSA will continue to work closely with industry stakeholders across all transportation modes to reduce cybersecurity risks and improve cyber resilience to support safe, secure and efficient travel," said TSA Administrator David Pekoske. "This amendment to the aviation security programs extends similar performance-based requirements that currently apply to other transportation system critical infrastructure."

TSA is taking this emergency action because of persistent cybersecurity threats against U.S. critical infrastructure, including the aviation sector. The new emergency amendment requires that impacted TSA-regulated entities develop an approved implementation plan that describes measures they are taking to improve their cybersecurity resilience and prevent disruption and degradation to their infrastructure. They must also proactively assess the effectiveness of these measures, which include the following actions:

1. Develop network segmentation policies and controls to ensure that operational technology systems 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. Implement continuous monitoring and detection policies and procedures to defend against, detect, and respond to cybersecurity threats and 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.

This is the latest in TSA's efforts to require that critical transportation sector operators continue to enhance their ability to defend against cybersecurity threats. Previous requirements for TSA-regulated airport and aircraft operators included measures such as reporting significant cybersecurity incidents to

the Cybersecurity and Infrastructure Security Agency (CISA), establishing a cybersecurity point of contact, developing and adopting a cybersecurity incident response plan and completing a cybersecurity vulnerability assessment.

On Thursday March 2, the Biden-Harris Administration announced the National Cybersecurity Strategy to secure the full benefits of a safe and secure digital ecosystem for all Americans. With this amendment and other ongoing efforts, TSA will continue to work closely with the Department of Transportation, CISA and industry partners to strengthen the cybersecurity resilience of the nation's critical infrastructure.

###

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.