Archived Content

In an effort to keep DHS.gov current, this document has been archived and contains outdated information that may not reflect current policy or programs.

FACT SHEET: TRANSPORTATION SPRINT
(SEPTEMBER – OCTOBER 2021)

OVERVIEW

In March 2021, Secretary of Homeland Security Alejandro N. Mayorkas outlined his vision for the Department's cybersecurity priorities in a virtual address. Secretary Mayorkas highlighted a series of focused 60-day sprints to operationalize his vision, drive action in the coming year, and raise public awareness about key cybersecurity priorities.

The Secretary's fourth 60-day sprint focused on the cybersecurity of the transportation sector. The sprint focused specifically on the need to increase the cyber resilience of the Nation's transportation systems – from aviation to rail, mass transit, pipelines, and the marine transportation system. These sprints are designed to (1) elevate existing work, (2) remove roadblocks to progress, and (3) launch new initiatives and partnerships to achieve DHS's cybersecurity mission and implement Biden-Harris Administration priorities. On October 6, Secretary Mayorkas gave a speech outlining DHS's actions as part of this 60-day sprint in more detail.

KEY FACTS AND OUTCOMES OF THE 60-DAY TRANSPORTATION SPRINT

- The Transportation Security Administration (TSA) issued two new Security Directives and updated its aviation security program requiring steps to strengthen cybersecurity across the transportation sector in response to significant and immediate cybersecurity threats. TSA also recommended additional guidance for voluntary measures for lower-risk surface transportation owners and operators to implement the same measures, namely (1) designating a cybersecurity coordinator, (2) reporting cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 24 hours, (3) developing an incident response and contingency plan, and (4) conducting a self-assessment.
- TSA announced its intent to initiate a rule-making process to increase the cybersecurity resiliency of the transportation sector in the medium- to long-term.
- The Coast Guard tasked the National Maritime Security Advisory Committee to provide recommendations on regulated vessel and facility vulnerability assessments occurring across the country, the Coast Guard's Maritime Cyber Risk Assessment Model, and potential improvements to cyber-related information sharing between the Coast Guard and industry.
- The Coast Guard initiated a Request for Information via the Federal Register to solicit public input for future regulatory steps regarding cyber risk management implementation aboard commercial vessels, facilities, and infrastructure in the areas of standards, regulatory barriers, and management.
- The Federal Emergency Management Agency (FEMA), in consultation with CISA, TSA, and the Coast Guard, updated its grant programs to support DHS's partners' efforts to strengthen cybersecurity in the transportation sector, including updating its Intercity Bus Security Grant Program, Intercity Passenger Rail, Port Security Grant Program, and Transit Security Grant Program.
- CISA produced a Vulnerability Insights report specifically focused on risks to the transportation sector and conducted threat briefings with industry organizations across the Aviation, Highway and Motor Carrier, Marine Transportation System, Mass Transit and Passenger Rail, and Freight Rail transportation sub-sectors.
- CISA promoted awareness of its Cyber Hygiene services with the transportation industry, which led to a 10.5% increase in adoption across the sector.
- Secretary Mayorkas engaged with industry leaders from across the maritime and aviation industries, including a roundtable discussion with Secretary of Transportation Pete Buttigieg and over a dozen executives from across the maritime industry on strengthening cybersecurity and resilience within the marine transportation system as well as meeting with CEOs and executives of major passenger and cargo airlines to discuss the importance of prioritizing cybersecurity.