

# Surface Transportation Security Awareness Message



## **ATTENTION—SURFACE TRANSPORTATION OWNER/OPERATORS**

Recent coordinated strikes against Iran and retaliatory missile attacks targeting U.S. and Israeli interests have increased the potential for threats to the homeland, including cyberattacks, acts of violence, and hate crimes. There are currently no specific credible threats to the homeland or surface transportation operations.

While there are no specific or credible threats to surface transportation at this time, TSA recommends that surface transportation stakeholders remain vigilant and ensure that all physical security measures and protocols are strictly followed. Foreign adversaries—including nation-state actors—may continue to seek opportunities to exploit current events, aiming to sow discord or inspire violence against transportation infrastructure, crowded places, or other soft targets.

In light of these circumstances, TSA recommends the following actions:

### **Recommended Actions:**

- Review plans and procedures for mitigation of common attack types, such as vehicle ramming, active shooter or edged weapon attacks, ransomware, or phishing.
- Remind employees, “If You See Something, Say Something®”, by reporting suspicious inquiries or activities in accordance with company policy.
- Review reporting procedures and ensure employees have updated instructions and contact information for company security personnel, local law enforcement, the [local FBI field office](#), and TSA’s Transportation Security Operations Center (TSOC) at 1-866-615-5150 to facilitate timely reporting of suspicious activities.

### **Resources:**

- Review Cybersecurity and Infrastructure Security Agency’s (CISA’s) [Be Air Aware](#) resource page, highlighting the use of Unmanned Aircraft Systems (UAS) and the significant threat they pose to critical infrastructure, their [Vehicle Ramming Mitigation](#) resource page, as well as [cybersecurity best practices](#) and [Shields Up](#) resource page for cybersecurity preparedness.
- Review the Federal Emergency Management Agency’s [Mass Gatherings: Security of Soft Targets and Crowded Places](#) resource guide as an operational tool to enhance detection capabilities and to identify suspicious activities.
- Further resources pertaining to trending threats can be found on the [Homeland Security Information Network \(HSIN\)](#).
- TSA’s Surface Information Sharing Cell (SISC) is a domestic (US only) surface transportation threat information-sharing and knowledge-management cell focusing on physical and cyber threats affecting all surface transportation modes. For more information and to join, see the attached SISC Fact Sheet and email: [siscops@tsa.dhs.gov](mailto:siscops@tsa.dhs.gov).
- TSA’s [First Observer Plus™ Program](#) provides transportation professionals with the knowledge needed to recognize suspicious activity possibly related to terrorism.

Thank you for your continued partnership in maintaining situational awareness and operational readiness during this current threat environment. Please feel free to share this awareness message within your organization.

*David W. Cooper*

David W. Cooper  
Executive Director (Acting), Surface Division  
Policy, Plans, and Engagement  
Transportation Security Administration  
Department of Homeland Security

