GAO Highlights

Highlights of GAO-20-404, a report to congressional addressees

April 2020

PASSENGER RAIL SECURITY

TSA Engages with Stakeholders but Could Better Identify and Share Standards and Key Practices

Why GAO Did This Study

Recent physical and cyberattacks on rail systems in U.S. and foreign cities highlight the importance of strengthening and securing passenger rail systems around the world. TSA is the primary federal agency responsible for securing transportation in the United States.

GAO was asked to review TSA's efforts to assess passenger rail risk, as well as its role in identifying and sharing security standards and key practices. This report addresses (1) TSA's efforts to assess risk; (2) the extent to which TSA works with U.S. and foreign passenger rail stakeholders to identify security standards and key practices; and (3) the extent to which TSA shares passenger rail security standards and key practices with stakeholders.

GAO analyzed TSA risk assessments from fiscal years 2015 through 2019 and reviewed TSA program documents and guidance. GAO interviewed officials from TSA, and from seven domestic rail agencies, three foreign rail agencies, and two foreign government agencies. The results from these interviews are not generalizable but provide perspectives on topics in this review.

What GAO Recommends

GAO is making two recommendations: (1) that TSA update TSAR guidance to include engaging with foreign passenger rail stakeholders; and (2) that TSA update the BASE cybersecurity questions to ensure they reflect key practices. DHS concurred with both recommendations.

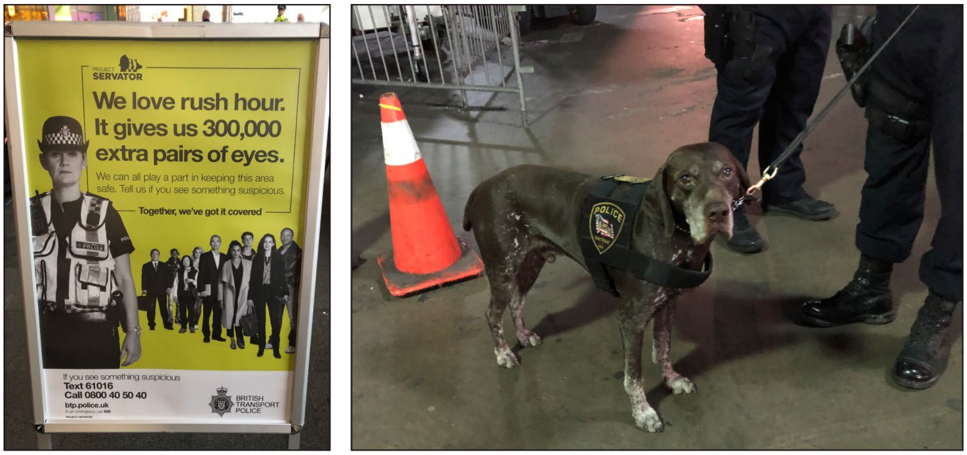
View GAO-20-404. For more information, contact Triana McNeil at (202) 512-8777 or mcneilt@gao.gov.

What GAO Found

The Transportation Security Administration (TSA) assesses passenger rail risks through the Transportation Sector Security Risk Assessment, the Baseline Assessment for Security Enhancement (BASE), and threat assessments. TSA uses the risk assessment to evaluate threat, vulnerability, and consequence for attack scenarios across various transportation modes. TSA surface inspectors use the baseline assessment, a voluntary security review for mass transit, passenger rail, and highway systems, to address potential vulnerabilities and share best practices, among other things.

TSA works with U.S. stakeholders to identify security standards and key practices and identifies foreign standards and practices through multilateral and bilateral exchanges. However, TSA Representatives (TSARs), the primary overseas point of contact for transportation security matters, lack specific guidance on foreign rail stakeholder engagement. As a result, TSA is less likely to be fully aware of key practices in other countries, such as station security guidance. Specific guidance would provide TSARs with clear expectations and encourage more consistent engagement with foreign rail stakeholders.

Examples of Security Key Practices Cited by Passenger Rail Stakeholders


PROJECT SERVATOR
We love rush hour.
It gives us 300,000 extra pairs of eyes.
We can all play a part in keeping this area safe. Tell us if you see something suspicious.
Together, we've got it covered
If you see something suspicious
Text 61016
Call 0800 40 50 40
btp.police.uk
BRITISH TRANSPORT POLICE
POLICE

Source: GAO. | GAO-20-404

Public Awareness Campaign
Emphasize security awareness

Canine Units
Detection of vapor from explosives

TSA shares standards and key practices with stakeholders, including those related to cybersecurity, through various mechanisms including BASE reviews; however, this assessment does not fully reflect current industry cybersecurity standards and key practices. For example, it does not include any questions related to two of the five functions outlined in the National Institute of Standards and Technology's Cybersecurity Framework—specifically the Detect and Recover functions. Updating the BASE questions to align more closely with this framework would better assist passenger rail operators in identifying current key practices for detecting intrusion and recovering from incidents.