



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

FOR IMMEDIATE RELEASE

Thursday, May 12, 2016

For Information Contact:

Public Affairs (202) 254-4100

New Report Finds IT Management Challenges Continue at TSA

The Department of Homeland Security (DHS) Office of Inspector General (OIG) today released a new report identifying IT security deficiencies related to screening equipment at our nation's airports.

In the report, *IT Management Challenges Continue in TSA's Security Technology Integrated Program*, OIG auditors describe weaknesses in the IT security controls of the Security Technology Integrated Program (STIP), a mission-essential data management system that connects airport transportation security equipment to servers. Connection to a centralized server allows remote management of passenger and baggage screening equipment and facilitates equipment maintenance, including software changes in response to emerging threats.

Persistent problems with STIP include unpatched software, inadequate contractor oversight, inadequate disaster recovery capability, physical security and environmental control deficiencies, and inadequate vulnerability reporting. These problems occurred because TSA typically has not managed STIP equipment in compliance with departmental guidelines regarding sensitive IT systems. TSA also did not effectively manage all IT components of STIP as IT investments and did not designate these assets as IT equipment. Thus, TSA did not ensure that IT security requirements were included in STIP procurement contracts, which promoted the use of unsupported operating systems that created security concerns and forced TSA to disconnect STIP equipment from the network. By August 2015, TSA had to disconnect STIP equipment from its network due to IT security concerns created by the unsupported operating systems. As of the end of our fieldwork in December 2015, the equipment was still disconnected.

Recently, TSA has taken significant steps to begin to resolve these STIP deficiencies. "TSA's proposed actions should resolve many of the STIP IT security deficiencies identified in this and prior OIG reports," said Inspector General John Roth. "We will continue to monitor the effectiveness of TSA's proposed improvements."

###

For more information visit our website, www.oig.dhs.gov