



### Why This Matters

Our audit of information technology (IT) security controls provide senior Department of Homeland Security (DHS) officials with timely information on whether they had properly implemented DHS IT security policies at critical sites. Our program is based on DHS Sensitive Systems Policy Directive 4300A, version 10 (DHS Directive 4300A), which applies to all DHS components. It provides direction to managers and senior executives regarding the management and protection of sensitive systems.

The three IT security areas audited were operational, management, and technical security controls.

### DHS Response

We obtained written comments on a draft of this report from the Assistant Director, Departmental GAO-OIG Audit Liaison. DHS concurred with 18 of the 19 recommendations. Additionally, the Department has already taken actions to resolve reported deficiencies. Further, TSA and ICE have provided documentation to support the resolution and closure of TSA's recommendation #2 and ICE's recommendations #15 and #18.

### For Further Information:

Contact our Office of Public Affairs at (202)254-4100, or email us at [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto:DHS-OIG.OfficePublicAffairs@oig.dhs.gov)

## Audit of Security Controls for DHS Information Technology Systems at Dallas/Fort Worth International Airport

### What We Determined

We audited technical and information security policies and procedures of Department of Homeland Security components at Dallas/Fort Worth International Airport (DFW). The Transportation Security Administration (TSA), U.S. Customs and Border Protection (CBP), and U.S. Immigration and Customs Enforcement (ICE) operate information technology systems that support homeland security operations at this airport.

Our audit focused on how these components had implemented computer security operational, management, and technical controls at the airport and nearby locations. We performed onsite audits of the areas where these assets were located, interviewed departmental staff, and conducted technical tests of internal controls. We also reviewed applicable policies, procedures, and other relevant documentation.

The information technology security controls implemented at these sites have deficiencies that, if exploited, could result in the loss of confidentiality, integrity, and availability of the components' respective information technology systems. For example, operational controls include physical security controls. At this airport there were two rooms with Transportation and Security Administration servers that were being used by unauthorized airline personnel.

### What We Recommend

We recommended that the Chief Information Officers for TSA, CBP, and ICE take steps to better implement DHS IT security policies in the areas of operational, management, and technical controls. Specifically, we made 7 recommendations to TSA; 4 recommendations to CBP; and 8 recommendations to ICE.

For example, based on our audit of operational controls, we recommended that TSA improve physical security and environmental controls for their server rooms. Additionally, we recommended that TSA and ICE improve the system security documentation for systems operating at DFW. Additionally, we recommended that all three components resolve high system vulnerabilities in a timely fashion.