



Why This Matters

We designed our Technical Security Evaluation Program to provide senior Department of Homeland Security (DHS) officials with timely information on whether they had properly implemented DHS information technology (IT) security policies at critical sites. Our program is based on DHS Sensitive Systems Policy Directive 4300A, version 9.1 (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 evaluated during our audit are technical, management, and operational 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 all 20 recommendations. Additionally, the Department has already taken actions to resolve reported deficiencies. Further, CBP and TSA have provided documentation to support the resolution and closure of recommendations 5 and 20, respectively.

For Further Information:

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

Technical Security Evaluation of DHS Activities Hartsfield-Jackson Atlanta International Airport

What We Determined

As part of our Technical Security Evaluation Program, we evaluated technical and information security policies and procedures of DHS components at Hartsfield-Jackson Atlanta International Airport (ATL). U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and the Transportation Security Administration (TSA) operate information technology systems that support homeland security operations at this airport.

Our evaluation focused on how these components had implemented computer security technical, management, and operational controls at the airport and nearby locations. We performed onsite inspections 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, a technical control includes regularly scanning servers for vulnerabilities.

What We Recommend

We recommended that the Chief Information Officers for CBP, ICE, and TSA take steps to better implement DHS IT security policies in the areas of technical, management and operational controls. Specifically, we made 6 recommendations to CBP; 8 recommendations to ICE; and 6 recommendations to TSA.

For example, based on our review of technical controls, we recommended that CBP, ICE, and TSA resolve high system vulnerabilities in a timely fashion. Based on our review of management controls, we also recommended that the components complete security authorization activities. Additionally, based on our review of operational controls, we recommended that the components assess whether it would be cost-effective to implement redundant communication circuits at some locations.