Spotlight
Department of Homeland Security
Office of Inspector General
March 2012 OIG-12-45

Technical Security Evaluation of DHS Activities at Chicago O'Hare International Airport

Why This Matters

Our Technical Security Evaluation Program provides senior Department of Homeland Security (DHS) officials with timely information on whether they had adequately implemented DHS Information Technology (IT) security policies at critical sites. Our program is based on DHS Sensitive Systems Policy Directive 4300A, which (1) applies to all DHS components and (2) 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 operational, technical, and management controls.

DHS Response

Transportation Security Administration (TSA) concurred with its four recommendations. We agree that TSA is taking steps to resolve these recommendations. U.S. Customs and Border Protection (CBP) concurred with its seven recommendations. We agree that CBP is taking steps to resolve four of its recommendations but we do not agree that CBP has addressed fully its remaining recommendations. U.S. Immigration and Customs Enforcement (ICE) concurred with one, and non-concurred with three recommendations. We agree that ICE is taking steps to resolve the one concurred recommendation and agree to close a second recommendation. We do not agree that the remaining two ICE recommendations should be closed.

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

What We Determined

As part of our Technical Security Evaluation Program, we evaluated technical and information security policies and procedures of DHS components at Chicago O'Hare International Airport. CBP, ICE and TSA operate information technology systems that support homeland security operations at this airport.

Our evaluation focused on how these components had implemented computer security operational, technical, and management 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' information technology systems. Specifically, these components need to improve their physical security and environmental controls for telecommunications equipment and servers. These components also need to improve their management controls by upgrading system information to more fully document security controls.

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 operational, technical, and management controls. Specifically, we made 3 operational control, 1 technical control, and 3 management control recommendations to CBP; 2 operational control and 2 management control recommendations to ICE; and 2 operational control, 1 technical control, and 1 management control recommendations to TSA.

For example, 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. Based on our review of technical controls, we also recommended that CBP and TSA perform vulnerability scans on specific systems. Additionally, based on our review of management controls, we recommended that the components prepare business impact assessments for systems operating at Chicago O'Hare International Airport.

The OIG considers recommendations #1 through #4, and #11 through #15 resolved; recommendations #5 through #8, and recommendation #10 are unresolved; and recommendation #9 closed.