IT Program Assessment
TSA – Secure Flight Program (2010)

Review Assessment

The DHS Chief Information Officer conducted a comprehensive program review of the TSA Secure Flight Program on January 6, 2010. TSA developed the Secure Flight Program to provide a watch list matching solution to fulfill the Congressional mandate and 9-11 Commission Report recommendation to pre-screen airline passengers against the terrorist watch list. Secure Flight operates under the TSA Transportation Threat Analysis Center (TTAC) and provides watch list matching for passengers traveling on covered airline flights into, out of, or within the U. S. and its territories, or over the continental Untied States, or between two international points where air travel is provided by covered U. S. airlines only, as well watch list matching for non-traveling individuals seeking authorization to enter the sterile area of an airport. Input to Secure Flight is from airline manifest, and persons listed on the manifest are matched against the terrorist watch list, the "No-Fly" list, and the selectee list. Secure Flight was initiated in 2004 and was approved for full operational capability in September 2009. The Secure Flight engaging with the airlines one at a time, and has a goal of vetting 2.5 million passengers per day by January 1, 2011.

Major findings during the DHS CIO IT Program Review of the Secure Flight Program include the following.

- The Secure Flight Program is working closely and effectively with the TSA TTAC IT Modernization Program to ensure program needs will be met going forward.
- The Secure Flight program is designed to provide common reusable service and assets such as security, identity management, monitoring, capacity management, telephone infrastructure, and systems engineering management tools.
- Secure Flight is Section 508 and NARA (National Archives and Records Administration) compliant, and reuse DHS capabilities including the DHS router for interface with airlines, and CBP ESTA program capabilities and components.
- With respect to COOP capabilities, Secure Flight has geographically redundant architecture with active-active configurations and backup power at both sites.
- There is some risk of single point of failure associated with the DHS router, which is the interface between TSA and CBP on the DHS side, and the airlines on the other side. TSA, CBP, and DHS are actively working to mitigate "single point of failure" risks with the DHS router.
- There is some programmatic but not-technical risk with non-US airlines and travel agencies being non-compliant with the requirements of the Secure Flight rule. Non-compliant submissions of information to Secure Flight could cause significantly higher false hits that have to be manually adjudicated. TSA is actively working this issue with the non-US airlines.
- No other significant program shortcomings or risks were identified.

Mitigation Strategy

Findings, issues, and risks from the DHS CIO IT Program Review of the Secure Flight program are being effectively addressed by the Secure Flight program and TSA management.

Score: 4