IT Program Assessment
Transportation Security Administration (TSA)
Information Technology Infrastructure Program

The Department of Homeland Security (DHS) Office of the Chief Information Officer (OCIO) conducted a program health review of the Transportation Security Administration (TSA) Information Technology Infrastructure Program (ITIP). This assessment represents the program's status through March 2012.

Description and Background:

The TSA ITIP program provides a communication and data processing platform used by all headquarters and TSA field elements in performing their mission of providing transportation security. ITIP includes email, database support, personal device communications, software and hardware refreshment, hotline, technical, and security support.

The program has migrated approximately 96% of its infrastructure to reside on the DHS consolidated Data Center 1 and 2, which is aligned with DHS's evolving cloud strategy. The users of the program include the entire TSA, Federal, state and local governments, airlines and other transportation industries, shipping entities, and the traveling public. Any TSA investment that depends upon communications or a secure and reliable database platform is dependent on ITIP.

Risks and Issues:

- If selected nodes on the TSAnet are not upgraded to allow for redundant operations, then the network could experience critical outages
- Currently, mobile technology and cloud computing products used by TSA personnel do not meet National Institute of Standard Technology Federal Information Processing Standard (NIST FIPS) security requirements.
- As stated in the previous assessment in September 2011, if program funding reductions come as expected, then the ability to ensure continuous growth with reliance on TSAnet requirements and uninterrupted service is jeopardized

ITIP has two issues: resources dependencies and vendor readiness:

- Entry-on-Duty (EOD) processing time for contracting staff ranges from 60 to 70 days and will delay the initial contractor start of work. These hiring delays negatively impact the program when staff is not 100% available at the start of the Period of Performance (PoP). The program is resolving this issue by frequent coordination meetings with TSA Office of Security as well as executing the EOD process at contract award.
- The skill level of support vendors does not match contract requirements. This adversely impacts the operational maintenance of the TSA Oracle database (DB). ITIP is resolving this issue by developing an extensive list of skills required for access and Operations and Maintenance on the TSA selected DB.

Mitigation Strategy:

The program will use the Defense Acquisition University (DAU) Planning, Programming, Budgeting, and Execution process to help manage major project priorities and mitigate the four risks cited above.

- The ITIP program will increase the priority for the TSAnet redundancy to provide higher network readiness and availability.
- TSA will participate in mobile technology or cloud computing with the DHS Integrated Product Team and other DHS action offices to gain lessons learned and ensure that mobile and cloud computing technology acceptance criteria meets the established NIST FIPS security requirements.
- ITIP Customer Relations Management is coordinating with the customer base for the insertion of new requirements. Also they are reviewing known customer requirements, to reduce duplication and multiple procurements for in scope and similar requirements. TSA aims to standardize and consolidate services and contracts as much as possible to reduce additional run-away costs.

Assessment:

The ITIP program improves operational effectiveness and business performance by providing continued IT Infrastructure services to users of the whole TSA Agency. The program has successfully migrated approximately 96% of its infrastructure to the DHS Data Center 1 and 2. However due to the high critical risks identified by the program such as unfavorable budget forecasts, possible network outages and mobile technology products not meeting security requirements. The CIO has assessed this program as a **Medium Risk**.

Score: 3