March 29, 2006

HOMELAND SECURITY

Progress Continues, but Challenges Remain on Department's Management of Information Technology

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-598T, a testimony before congressional subcommittees

Why GAO Did This Study

Information technology (IT) is a critical tool for the Department of Homeland Security (DHS), not only in performing its mission today, but also in transforming how it will do so in the future. In light of the importance of this transformation and the magnitude of the associated challenges, GAO has designated the implementation of the department and its transformation as high risk.

GAO has reported that in order to effectively leverage IT as a transformation tool, DHS needs to establish certain institutional management controls and capabilities, such as having an enterprise architecture and making informed portfolio-based decisions across competing IT investments. GAO has also reported that it is critical for the department to implement these controls and associated best practices on its many IT investments.

In its past work, GAO has made numerous recommendations on DHS institutional controls and on individual IT investment projects. The testimony is based on GAO's body of work in these areas, covering the state of DHS IT management both on the institutional level and the individual program level.

www.gao.gov/cgi-bin/getrpt?GAO-06-598T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov.

What GAO Found

DHS continues to work to institutionalize IT management controls and capabilities (disciplines) across the department. Among these are

- having and using an enterprise architecture, or corporate blueprint, as an authoritative frame of reference to guide and constrain IT investments;
- defining and following a corporate process for informed decision making by senior leadership about competing IT investment options;
- applying system and software development and acquisition discipline and rigor when defining, designing, developing, testing, deploying, and maintaining systems;
- establishing a comprehensive information security program to protect its information and systems;
- having sufficient people with the right knowledge, skills, and abilities to execute each of these areas now and in the future; and
- centralizing leadership for extending these disciplines throughout the organization with an empowered Chief Information Officer.

Over the last 3 years, the department has made efforts to establish and implement these IT management disciplines, but it has more to do. Despite progress, for instance, in developing its enterprise architecture and its investment management processes, much work remains before these and the other disciplines are fully mature and institutionalized. For example, although the department recently completed a comprehensive inventory of its major information systems—a prerequisite for effective security management—it has not fully implemented a comprehensive information security program, and its other institutional IT disciplines are still evolving. The department also has more to do in deploying and operating IT systems and infrastructure in support of core mission operations, such as border and aviation security. For example, a system to identify and screen visitors entering the country has been deployed and is operating, but a related exit capability largely is not. Also, a government-run system to prescreen domestic airline passengers is not yet in place. Similarly, some infrastructure has been delivered, but goals related to consolidating networks and e-mail systems, for example, remain to be fully accomplished.

Similarly, GAO's review of key nonfinancial systems show that DHS has more to do before the IT disciplines discussed above are consistently employed. For example, these programs have not consistently employed reliable cost estimating practices, effective requirements development and test management, meaningful performance measurement, strategic workforce management, and proactive risk management, among other recognized program management best practices.

Until the department fully establishes and consistently implements the full range of IT management disciplines embodied in best practices and federal guidance, it will be challenged in its ability to manage and deliver programs.