September 2008

SECURE BORDER INITIATIVE

DHS Needs to Address Significant Risks in Delivering Key Technology Investment

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-08-1086, a report to congressional requesters

Why GAO Did This Study

The Department of Homeland Security's (DHS) Secure Border Initiative (SBI) is a multiyear, multibillion-dollar program to secure the nation's borders through, among other things, new technology, increased staffing, and new fencing and barriers. The technology component of SBI, which is known as SBI*net*, involves the acquisition, development, integration, and deployment of surveillance systems and command, control, communications, and intelligence technologies. GAO was asked to determine whether DHS (1) has defined the scope and timing of SBI*net* capabilities and how these capabilities will be developed and deployed, (2) is effectively defining and managing SBI*net* requirements, and (3) is effectively managing SBI*net* testing. To do so, GAO reviewed key program documentation and interviewed program officials, analyzed a random sample of requirements, and observed operations of a pilot project.

What GAO Recommends

GAO is recommending that DHS assess and disclose the risks associated with its planned SBI*net* development, testing, and deployment activities, and address the system deployment, requirements management, and testing weaknesses that GAO identified. DHS agreed with all but one of GAO's eight recommendations and described actions completed, underway, and planned to address them.

To view the full product, including the scope and methodology, click on GAO-08-1086. For more information, contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov.

What GAO Found

Important aspects of SBI*net* remain ambiguous and in a continued state of flux, making it unclear and uncertain what technology capabilities will be delivered, when and where they will be delivered, and how they will be delivered. For example, the scope and timing of planned SBI*net* deployments and capabilities have continued to change since the program began and, even now, are unclear. Further, the program office does not have an approved integrated master schedule to guide the execution of the program, and GAO's assimilation of available information indicates that the schedule has continued to change. This schedule-related risk is exacerbated by the continuous change in and the absence of a clear definition of the approach that is being used to define, develop, acquire, test, and deploy SBI*net*. The absence of clarity and stability in these key aspects of SBI*net* impairs the ability of the Congress to oversee the program and hold DHS accountable for program results, and it hampers DHS's ability to measure program progress.

SBI*net* requirements have not been effectively defined and managed. While the program office recently issued guidance that defines key practices associated with effectively developing and managing requirements, such as eliciting user needs and ensuring that different levels of requirements and associated verification methods are properly aligned with one another, the guidance was developed after several key activities had been completed. In the absence of this guidance, the program has not effectively performed key requirements definition and management practices. For example, it has not ensured that different levels of requirements are properly aligned, as evidenced by GAO's analysis of a random probability sample of component requirements showing that a large percentage of them could not be traced to higher-level system and operational requirements. Also, some of SBI*net*'s operational requirements, which are the basis for all lower-level requirements, were found by an independent DHS review to be unaffordable and unverifiable, thus casting doubt on the quality of lower-level requirements that are derived from them. As a result, the risk of SBI*net* not meeting mission needs and performing as intended is increased, as are the chances of expensive and time-consuming system rework.

SBI*net* testing has not been effectively managed. For example, the program office has not tested the individual system components to be deployed to the initial deployment locations, even though the contractor initiated integration testing of these components with other system components and subsystems in June 2008. Further, while a test management strategy was drafted in May 2008, it has not been finalized and approved, and it does not contain, among other things, a clear definition of testing roles and responsibilities; a high-level master schedule of SBI*net* test activities; or sufficient detail to effectively guide project-specific test planning, such as milestones and metrics for specific project testing. Without a structured and disciplined approach to testing, the risk that SBI*net* will not satisfy user needs and operational requirements, thus requiring system rework, is increased.