United States Government Accountability Office

GAO

Testimony Before the Subcommittees on Management, Investigations, and Oversight; and Border, Maritime, and Global Counterterrorism; Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EST
Thursday, June 17, 2010

SECURE BORDER INITIATIVE

DHS Needs to Follow Through on Plans to Reassess and Better Manage Key Technology Program

Statement of Randolph C. Hite, Director
Information Technology Architecture and System Issues

GAO
Accountability ★ Integrity ★ Reliability

June 17, 2010

Messrs. Chairmen and Members of the Subcommittees:

I appreciate the opportunity to participate in today's hearing on the technology component of the Department of Homeland Security's (DHS) Secure Border Initiative (SBI). My statement today is based on our report, *Secure Border Initiative: DHS Needs to Reconsider Its Proposed Investment in Key Technology Program*, which is being released at this hearing.[1]

As you know, SBI is intended to help secure the 6,000 miles of international borders that the contiguous United States shares with Canada and Mexico. The program, which began in November 2005, seeks to enhance border security and reduce illegal immigration by improving surveillance technologies, raising staffing levels, increasing domestic enforcement of immigration laws, and improving physical infrastructure along the nation's borders. Within SBI, the Secure Border Initiative Network (SBI*net*) is a multibillion dollar program that includes the acquisition, development, integration, deployment, and operation of surveillance technologies—such as unattended ground sensors and radar and cameras mounted on fixed and mobile towers—to create a "virtual border fence." In addition, command, control, communications, and intelligence (C3I) software and hardware are to use the information gathered by the surveillance technologies to create a real-time picture of what is transpiring within specific areas along the border and transmit the information to command centers and vehicles.

Since 2007, we have identified a range of management weaknesses and risks facing SBI*net*, and we have made a number of recommendations to address them that DHS has largely agreed with and, to varying degrees, taken actions to address. Recently, in September 2008, we reported that important aspects of SBI*net* were still ambiguous and in a continuous state of flux 3 years after the program began, making it unclear and uncertain

[1] GAO-10-340 (Washington, D.C.: May 5, 2010). Both the report and this statement are based on work performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained during the course of this review does provide a reasonable basis for our findings and conclusions based on our audit objectives.

what technology capabilities were to be delivered when.[2] In addition, the program still lacked an approved schedule to guide its execution, and key milestones continued to slip. This schedule-related risk was exacerbated by the absence of a clearly defined approach used for developing and deploying SBI*net*. Furthermore, different levels of SBI*net* requirements were not properly aligned, and not all requirements had been properly defined and validated. Also, the program office was not effectively managing early test events. We thus emphasized at that time that the program was not on a path for success and that change was needed. In March 2010, we reported that recently completed test events were not adequate, as illustrated by poorly defined test plans and numerous and extensive last-minute changes to test procedures, and we reported on a growing number of system performance and quality problems, which we said was not indicative of a maturing system.[3] We have also reported multiple times on the impact that SBI*net* performance limitations have had on Border Patrol operations. In particular, we reported that the instability of the cameras, mechanical problems with the tower-mounted radar, and the sensitivity of the radar have limited system reliability and contributed to significant delays in system deployment along the southwest border. As a result, Border Patrol agents have been forced to rely on existing technologies that have their own limitations, such as cameras mounted on towers that intermittently lose signals.[4]

My statement today summarizes our most recent report on SBI*net*, which is being released publicly at this hearing. In summary, the report provided a timely and compelling case for DHS to rethink the plans it had in place at the beginning of this year for investing in SBI*net*. In this regard, we showed that the scope of the initial system's capabilities and areas of deployment have continued to shrink, thus making it unclear what capabilities are to be delivered when. Moreover, DHS had yet to demonstrate the cost-effectiveness of the proposed SBI*net* solution, and thus whether the considerable time and money being invested represented a prudent use of limited resources. Further, DHS had not employed the

[2] GAO, *Secure Border Initiative: DHS Needs to Address Significant Risks in Delivering Key Technology Investment*, GAO-08-1086 (Washington, D.C.: Sept. 22, 2008).

[3] GAO, *Secure Border Initiative: Testing and Problem Resolution Challenges Put Delivery of Technology Program at Risk*, GAO-10-511T (Washington, D.C.: Mar. 18, 2010).

[4] See, for example, GAO, *Secure Border Initiative: DHS Has Faced Challenges Deploying Technology and Fencing Along the Southwest Border*, GAO-10-651T (Washington, D.C.: May 4, 2010).

kind of acquisition management rigor and discipline needed to reasonably ensure that the proposed system capabilities would be delivered on time and within budget. Collectively, we concluded that these limitations increased the risk that the proposed solution would not meet the department's stated border security and immigration management goals. To minimize the program's exposure to risk, we recommended that DHS determine whether its proposed SBI*net* solution satisfied the department's border security needs in the most cost-effective manner and that the department improve several key life cycle management areas. DHS largely agreed with our recommendations. More importantly, since receiving these recommendations in a draft of our report in March 2010, the Secretary of Homeland Security has taken action to limit the department's near-term investment in SBI*net* pending its completion of an analysis of alternative investment options. This and other planned actions are consistent with the intent of our recommendations.

Background

Managed by DHS's Customs and Border Protection (CBP), SBI*net* is intended to strengthen CBP's ability to detect, identify, classify, track, and respond to illegal breaches at and between ports of entry. The SBI Program Executive Office, which is organizationally within CBP, is responsible for managing key acquisition functions associated with SBI*net*, such as requirements management and risk management. Within the Executive Office, the SBI*net* System Program Office (SPO) is responsible for managing the day-to-day development and deployment of SBI*net*.

In September 2006, CBP awarded a 3-year contract to the Boeing Company for SBI, with three additional 1-year options. As the prime contractor, Boeing is responsible for designing, producing, testing, deploying, and sustaining the system. In September 2009, CBP extended its contract with Boeing for the first option year. CBP is acquiring SBI*net* incrementally in a series of discrete units of capabilities, referred to as "blocks." Each block is to deliver one or more system capabilities from a subset of the total system requirements. The first block, known as Block 1, is to include a mix of surveillance technologies (e.g., cameras, radars, and sensors) and C3I technologies that are to produce a common operating picture—a uniform presentation of activities within specific areas along the border. Block 1 is to be initially deployed within the Tucson Sector to the Tucson Border Patrol Station (TUS-1) and to the Ajo Border Patrol Station (AJO-1). As of

May 2010, the TUS-1 system is scheduled for government acceptance in September 2010, with AJO-1 acceptance in November 2010.[5]

In January 2010, the DHS Secretary ordered a departmentwide reassessment of the program to include a comprehensive assessment of alternatives to SBI*net* to ensure that the department utilizes the most efficient and effective technological and operational solutions to secure the border. Pending the results of the assessment, the Secretary also froze all Block 1 expenditures beyond those needed to complete the implementation of the initial SBI*net* deployments to TUS-1 and AJO-1. Further, in March 2010, the department announced its plans to redeploy $50 million from its American Recovery and Reinvestment Act of 2009 funding to purchase currently available, stand-alone technology, such as remote-controlled camera systems called Remote Video Surveillance Systems, and truck-mounted systems with cameras and radar, called Mobile Surveillance Systems, to meet near-term operational needs.

Block 1 Capabilities, Geographic Coverage, and Performance Standards Have Continued to Decrease

In order to measure system acquisition progress and promote accountability for results, organizations need to establish clear commitments around what system capabilities will be delivered, and when and where they will be delivered. In September 2008, we reported that the scope of SBI*net* was becoming more limited without becoming more specific, thus making it unclear and uncertain what system capabilities would be delivered when and to what locations.[6] Accordingly, we recommended that DHS establish and baseline the specific program commitments, including the specific system functional and performance capabilities that are to be deployed to the Tucson, Yuma, and El Paso Sectors, and establish when these capabilities are to be deployed and are to be operational.

To its credit, the SPO subsequently defined the scope of the first incremental block of SBI*net* capabilities that it intended to deploy and make operational; however, these capabilities and the number of geographic locations to which they are to be deployed have continued to shrink. For example, the number of component-level requirements[7] to be

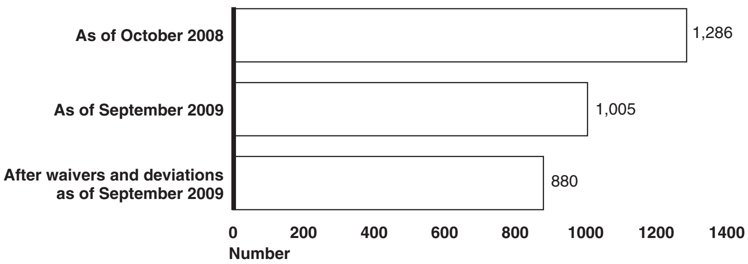
[5] This schedule has yet to be approved by CBP.

[6] GAO-08-1086.

[7] Component-level requirements describe required features of various surveillance components (e.g., cameras and radars) and infrastructure (e.g., communications).

deployed to the TUS-1 and AJO-1 locations has decreased by about 32 percent since October 2008 (see fig. 1).

Figure 1: Illustration of Reduction in Block 1 Requirements from October 2008 through September 2009



Source: GAO analysis of DHS data.

In addition, the number of sectors that the system is to be deployed to was reduced from three border sectors spanning about 655 miles to two sectors spanning about 387 miles. Further, the stringency of the performance measures was relaxed, to the point that system performance is now deemed acceptable if it identifies less than 50 percent of items of interest that cross the border. According to program officials, the decreases are due to poorly defined requirements and limitations in the capabilities of commercially available system components. The result will be a deployed and operational system that does not live up to user expectations and provides less mission support than was envisioned.

A Reliable Schedule for Completing Block 1 Has Not Been Developed

The success of a large-scale system acquisition program, like SBI*net*, depends in part on having a reliable schedule of when the program's set of work activities and milestone events will occur, how long they will take, and how they are related to one another. Among other things, a reliable schedule provides a road map for systematic execution of a program and the means by which to gauge progress, identify and address potential problems, and promote accountability. In September 2008, we reported that the program did not have an approved master schedule that could be used to guide the development of SBI*net*. Accordingly, we recommended that the SPO finalize and approve an integrated master schedule that reflects the timing and sequencing of SBI*net* tasks.

However, DHS has yet to develop a reliable integrated master schedule for delivering the first block of SBI*net*. Specifically, the August 2009 SBI*net* integrated master schedule, which was the most current version available at the time of our review, did not sufficiently comply with seven of nine schedule estimating practices that relevant guidance[8] states are important to having a reliable schedule.[9] For example, the schedule did not adequately capture all necessary activities to be performed, including those to be performed by the government, such as obtaining environmental permits in order to construct towers. Further, the schedule did not include a valid critical path, which represents the chain of dependent activities with the longest total duration in the schedule, and it does not reflect a schedule risk analysis, which would allow the program to better understand the schedule's vulnerability to slippages in the completion of tasks.

These limitations are due, in part, to the program's use of the prime contractor to develop and maintain the integrated master schedule, whose processes and tools do not allow it to include in the schedule work that it does not have under contract to perform, as well as the constantly changing nature of the work to be performed. Without having a reliable schedule, it is unclear when the first block will be completed, and schedule delays are likely to continue.

Cost-Effectiveness of Block 1 Has Not Been Demonstrated

The decision to invest in any system, or major system increment, should be based on reliable estimates of costs and meaningful forecasts of quantifiable and qualitative benefits over the system's useful life. However, DHS has not demonstrated the cost-effectiveness of Block 1. In particular, it has not reliably estimated the costs of this block over its entire life cycle. To do so requires DHS to ensure that the estimate meets key practices that relevant guidance[10] states are important to having an estimate that is comprehensive, well-documented, accurate, and credible. However, DHS's cost estimate for Block 1, which is about $1.3 billion, does not sufficiently possess any of these characteristics.

[8] GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP (Washington, D.C.: March 2009), 218–224.

[9] These are (1) capturing all activities, (2) sequencing all activities, (3) assigning resources to all activities, (4) establishing the duration of all activities, (5) integrating activities horizontally and vertically, (6) establishing the critical path for all activities, (7) identifying reasonable float between activities, (8) conducting a schedule risk analysis, and (9) updating the schedule using logic and durations.

[10] GAO-09-3SP, 8–13.

Further, DHS has yet to identify expected quantifiable or qualitative benefits from this block and analyze them relative to costs. According to program officials, it is premature to project such benefits given the uncertainties surrounding the role that Block 1 will ultimately play in overall border control operations, and that operational experience with Block 1 is first needed in order to estimate such benefits. While we recognize the value of operationally evaluating an early, prototypical version of a system in order to better inform investment decisions, we question the basis for spending in excess of a billion dollars to gain this operational experience. Without a meaningful understanding of SBI*net* costs and benefits, DHS lacks an adequate basis for knowing whether the initial system solution is cost-effective.

Block 1 Has Not Been Managed in Accordance with Key Life Cycle Management Processes

Successful management of large information technology programs, like SBI*net*, depends in large part on having clearly defined and consistently applied life cycle management processes. In September 2008, we reported that the SBI*net* life cycle management approach had not been clearly defined. Accordingly, we recommended that the SPO revise, approve, and implement its life cycle management approach, including implementing key requirements development and management practices, to reflect relevant federal guidance and leading practices. To the SPO's credit, it has defined key life cycle management processes that are largely consistent with relevant guidance and associated best practices. However, it has not effectively implemented these processes. In particular:

- The SPO revised its Systems Engineering Plan, which documents its life cycle management approach for SBI*net* definition, development, testing, deployment, and sustainment, in November 2008, and this plan is largely consistent with DHS and other relevant guidance. For example, it defines a number of key life cycle milestone or "gate" reviews that are important in managing the program, such as initial planning reviews, requirements reviews, system design reviews, and test reviews. The plan also requires most key artifacts and program documents that DHS guidance identified as important to each gate review, such as a risk management plan and requirements documentation. However, the SPO has not consistently implemented these life cycle management activities for Block 1. For example, the SPO did not review or consider key artifacts, including plans for testing and evaluating the performance of the system, as well as assessing the robustness of the system's security capabilities, during its Critical Design Review, which is the point when, according to the plan, verification and testing plans are to be in place.

- The SBI*net* Requirements Development and Management Plan states that (1) a baseline set of requirements should be established by the time of the Critical Design Review; (2) requirements should be achievable, verifiable, unambiguous, and complete; and (3) requirements should be bi-directionally traceable from high-level operational requirements through detailed low-level requirements to test plans. Further, the plan states that ensuring traceability of requirements from lower-level requirements to higher-level requirements is an integral part of ensuring that testing is properly planned and conducted. However, not all Block 1 component requirements were sufficiently defined at the time that they were baselined at the Critical Design Review. Further, operational requirements continue to be unclear and unverifiable, which has contributed to testing challenges, including the need to extemporaneously rewrite test cases during test execution. In addition, while requirements are now largely traceable backwards to operational requirements and forward to design requirements and verification methods, this traceability has not been used until recently to verify that higher-level requirements have been satisfied.

- In 2008, the SPO documented a risk management approach that largely complies with relevant guidance. However, it has not effectively implemented this approach for all risks. Moreover, available documentation does not demonstrate that significant risks were disclosed to DHS and congressional decision makers in a timely fashion as we previously recommended, and, while risk disclosure to DHS leadership has recently improved, not all risks have been formally captured and thus shared. For example, some of the risks that have not been formally captured include the lack of well-defined acquisition management processes, staff with the appropriate acquisition expertise, and agreement on key system performance parameters. However, the SPO recently established a risk management process for capturing SBI enterprisewide risks, including the lack of well-defined acquisition management processes and staff expertise.

Reasons cited by program officials for not implementing these processes include their decision to rely on task order requirements that were developed prior to the Systems Engineering Plan and competing SPO priorities, including meeting an aggressive deployment schedule. Until the SPO consistently implements these processes, it will remain challenged in its ability to successfully deliver SBI*net*.

DHS Has Agreed to Implement GAO Recommendations Aimed at Addressing SBI*net* Longstanding Uncertainties and Risks

To address the program's risks, uncertainties, and acquisition management weaknesses, our report being released today provides 12 recommendations.

In summary, we recommended that DHS limit future investment in SBI*net* to work that is either already under contract and supports the completion of Block 1 activities for deployment to TUS-1 and AJO-1 and/or provides a basis for a departmental decision on what, if any, expanded investment in SBI*net* is justifiable as a prudent use of DHS's resources for carrying out its border security and immigration management mission. As part of this recommendation, we reiterated prior recommendations pertaining to program management challenges and recommended that DHS address weaknesses identified in our report by, for example, ensuring that the SBI*net* integrated master schedule, Block 1 requirements, and the Systems Engineering Plan, among other program elements, are consistent with best practices.

We also recommended that the program undertake a detailed cost-benefit analysis of any incremental block of SBI*net* capabilities beyond Block 1 and report the results of such analyses to CBP and DHS leadership. Further, we recommended that DHS decide whether proceeding with expanded investment in SBI*net* represents a prudent use of the department's resources, and report the decision, and the basis for it, to the department's authorization and appropriations committees.

To DHS's credit, it has initiated actions to address our recommendations. In particular, and as previously mentioned, the department froze all funding beyond the initial TUS-1 and AJO-1 deployments until it completes a comprehensive reassessment of the program that includes an analysis of the cost and projected benefits of additional SBI*net* deployments, as well as the cost and mission effectiveness of alternative technologies.

Further, in written comments on a draft of our report, DHS described steps it is taking to fully incorporate best practices into its management of the program. For example, DHS stated that, in response to our previous recommendations, it has instituted more rigorous oversight of SBI*net*, requiring the program to report to the department's Acquisition Review Board at specified milestones and receive approval before proceeding with the next deployment increment. With respect to our new recommendations, DHS stated that it is, among other things, taking steps to bring the Block 1 schedule into alignment with best practices, verifying requirements and validating performance parameters, updating its Systems Engineering Plan, and improving its risk management process.

In closing, let me emphasize our long held position that SBI*net* is a risky program. To minimize the program's exposure to risk, it is imperative for DHS to follow through on its stated commitment to ensure that SBI*net*, as proposed, is the right course of action for meeting its stated border security and immigration management goals and outcomes, and once this is established, for it to ensure that the program is executed in accordance with proven acquisition management best practices. To do less will perpetuate a program that has for too long been oversold and under delivered.

This concludes my prepared statement. I would be pleased to respond to any questions that you or other Members of the Subcommittees may have.

Contact and Staff Acknowledgments

For questions about this statement, please contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this testimony. Individuals making key contributions to this testimony include Deborah Davis, Assistant Director; David Alexander; Rebecca Alvarez; Carl Barden; Sylvia Bascopé; Tisha Derricotte; Neil Doherty; Nancy Glover; Dan Gordon; Cheryl Dottermusch; Thomas J. Johnson; Kaelin P. Kuhn; Jason T. Lee; Jeremy Manion; Taylor Matheson; Lee McCracken; Jamelyn Payan; Karen Richey; Karl W.D. Seifert; Matt Snyder; Sushmita Srikanth; Jennifer Stavros-Turner; Stacey L. Steele; Karen Talley; and Juan Tapia-Videla.

(310687)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548