United States Government Accountability Office

GAO

Testimony Before the Committee on Homeland Security's Subcommittees on Management, Investigations, and Oversight; and Border, Maritime, and Global Counterterrorism

For Release on Delivery
Expected at 10:00 a.m. EDT,
Thursday, March 18, 2010

SECURE BORDER INITIATIVE

Testing and Problem Resolution Challenges Put Delivery of Technology Program at Risk

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

March 18, 2010

Mr. Chairman and Members of the Subcommittees:

Thank you for 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 Address Testing and Performance Limitations That Place Key Technology Program at Risk*, 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 fence" along the border. In addition, command, control, communications, and intelligence software and hardware are to use the information gathered by the surveillance technologies to create a common operating picture (COP) of activities within specific areas along the border and transmit the information to command centers and vehicles.

[1]GAO-10-158 (Washington, D.C.: Jan. 29, 2010). Both the report and this statement are based on work performed in accordance with generally accepted government 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.

In September 2008, we reported to you that important aspects of SBI*net* were ambiguous and in a continuous state of flux, making it unclear and uncertain what technology capabilities were to be delivered when. In addition, the program did not have an approved integrated master schedule to guide the program's execution, and key milestones continued to slip. This schedule-related risk was exacerbated by the continuous change in and the absence of a clear definition of the approach used to define, develop, acquire, test, and deploy SBI*net*. Furthermore, different levels of SBI*net* requirements were not properly aligned, and all requirements had not been properly defined and validated. Also, the program office had not tested the individual system components to be deployed to initial locations, even though the contractor had initiated integration testing of these components with other system components and subsystems, and its test management strategy did not contain, among other things, a clear definition of testing roles and responsibilities; or sufficient detail to effectively guide planning for specific test events, such as milestones and metrics. Accordingly, we made recommendations to address these weaknesses which DHS largely agreed to implement.[2]

In light of SBI*net*'s important mission, high cost, and risks, you asked us to conduct a series of four SBI*net* reviews. This statement and report being released today provide the results for the first of these reviews.[3] Specifically, they address (1) the extent to which SBI*net* testing has been effectively managed, including identifying the types of tests performed and whether they were well planned and executed; (2) what the results of testing show; and (3) what processes are being used to test and incorporate maturing technologies into SBI*net*.

In summary, SBI*net* testing has not been adequately managed, as illustrated by poorly defined test plans and numerous and extensive last-minute changes to test procedures. Further, testing that has been performed identified a growing number of system performance

[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]See attachment 1 for the objectives and status of the other three reviews.

and quality problems—a trend that is not indicative of a maturing system that is ready for deployment anytime soon. Further, while some of these problems have been significant, the collective magnitude of the problems is not clear because they have not been prioritized, user reactions to the system continue to raise concerns, and key test events remain to be conducted. Collectively, these limitations increase the risk that the system will ultimately not perform as expected and will take longer and cost more than necessary to implement. For DHS to increase its chances of delivering a version of SBI*net* for operational use, we are recommending that DHS improve the planning and execution of future test events and the resolution and disclosure of system problems. DHS agreed with our recommendations.

Background

Managed by DHS's Customs and Border Protection (CBP), SBI*net* is to strengthen CBP's ability to detect, identify, classify, track, and respond to illegal breaches at and between ports of entry. CBP's SBI Program Office is responsible for managing key acquisition functions associated with SBI*net*, including tracking and overseeing the prime contractor.

In September 2006, CBP awarded a 3-year contract to the Boeing Company for SBI*net*, 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.

In August 2008, the DHS Acquisition Review Board decided to delay the initial deployment of Block 1 of SBI*net* so that fiscal year 2008 funding could be reallocated to complete physical infrastructure projects. In addition, the board directed the SBI*net* System Program Office (SPO) to deliver a range of program documentation, including

an updated Test and Evaluation Master Plan (TEMP),[4] detailed test plans, and a detailed schedule for deploying Block 1 to two initial sites in the Tucson Sector of the southwest border. This resulted in a revised timeline for deploying Block 1, first to the Tucson Border Patrol Station (TUS-1) in April 2009, and then to the Ajo Border Patrol Station (AJO-1) in June 2009. Together, these two deployments are to cover 53 miles of the 1,989-mile-long southern border. However, the SBI Executive Director told us in December 2009 that these and other SBI*net* scheduled milestones were being reevaluated. As of January 2010, the TUS-1 system is scheduled for government acceptance in September 2010, with AJO-1 acceptance in November 2010. However, this schedule has yet to be approved by CBP.

DHS Has Not Effectively Managed SBI*net* Testing

Testing is essential to knowing whether the system meets defined requirements and performs as intended. Effective test management involves, among other things, developing well-defined test plans and procedures to guide test execution. It is intended to identify and resolve system quality and performance problems as early as possible in the system development life cycle.

DHS has not effectively managed key aspects of SBI*net* testing, which has in turn increased the risk that the system will not perform as expected and will take longer and cost more than necessary. While the department's testing approach appropriately consists of a series of progressively expansive test events, some of which have yet to be completed, test plans and test cases for recently executed test events were not defined in accordance with relevant guidance. For example, none of the plans for tests of system components addressed testing risks and mitigation strategies.

[4]The TEMP defines the program's integrated test and evaluation approach, including the scope of testing and the staff, resources (equipment and facilities), and funding requirements associated with testing.

Further, SBI*net* test procedures were generally not executed as written. Specifically, about 70 percent of the procedures for key test events were rewritten extemporaneously during execution because persons conducting the tests determined that the approved procedures were not sufficient or accurate. Moreover, changes to these procedures were not made according to a documented quality assurance process but were instead made based on an undocumented understanding that program officials said they established with the contractor. While some of these changes were relatively minor, others were significant, such as adding requirements or completely rewriting verification steps. The volume and nature of the changes made to the test procedures, in conjunction with the lack of a documented quality assurance process, increases the risk that system problems may not be discovered until later in the sequence of testing. This concern is underscored by a program office letter to the prime contractor stating that changes made to system qualification test procedures appeared to be designed to pass the test instead of being designed to qualify the system.

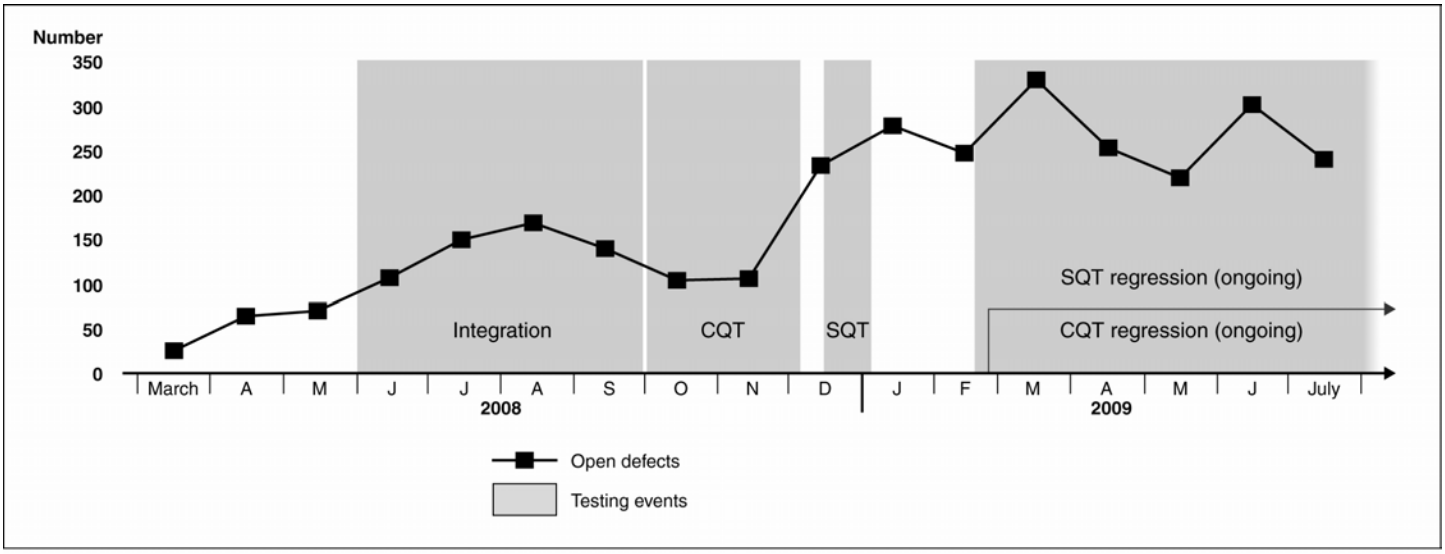
These limitations are due, among other things, to a lack of detailed guidance in the TEMP, the program's aggressive milestones, schedule, and ambiguities in requirements. Collectively, these limitations increase the likelihood that testing will not discover system issues or demonstrate the system's ability to perform as intended.

SBI*net* Testing Results Have Identified a Growing Number of System Performance and Quality Problems

The number of new SBI*net* defects that have been discovered during testing has increased faster than the number that has been fixed. (See figure 1 for the trend in the number of open defects from March

2008 to July 2009.) As we previously reported[5] such an upward trend is indicative of an immature system.

Figure 1: SBI*net* Open Defects from March 2008 to July 2009



Source: GAO analysis of DHS data.

Some of the defects found during testing have been significant, prompting the DHS Acquisition Review Board in February 2009 to postpone deployment of Block 1 capabilities to TUS-1 and AJO-1. These defects included the radar circuit breaker frequently tripping when the radar dish rotated beyond its intended limits, COP workstations crashing, and blurry camera images, among others.

While program officials have characterized the defects and problems found during development and testing as not being "show stoppers," they have nevertheless caused delays, extended testing, and required time and effort to fix. Moreover, the SPO and its contractor have continued to find problems that further impact the program's schedule. For example, the radar problems mentioned previously were addressed by installing a workaround that included

[5]GAO, *Office of Personnel Management: Improvements Needed to Ensure Successful Retirement Systems Modernization*, GAO-08-345 (Washington, D.C.: Jan. 31, 2008).

a remote ability to reactivate the circuit breaker via software, which alleviated the need to send maintenance workers out to the tower to manually reset the circuit. However, this workaround did not fully resolve the problem, and program officials said that root cause analysis continues on related radar power spikes and unintended acceleration of the radar dish that occasionally render the system inoperable. One factor that has contributed to the time and resources needed to resolve this radar problem, and potentially other problems, is the ability of the prime contractor to effectively determine root causes for defects. According to program officials, including the SBI Executive Director, the contractor's initial efforts to isolate the cause of the radar problems were flawed and inadequate. Program officials added, however, that they have seen improvements in the contractor's efforts to resolve technical issues.

Along with defects revealed by system testing, Border Patrol operators participating in an April 2009 user assessment identified a number of concerns. During the assessment, operators compared the performance of Block 1 capabilities to those of existing technologies. While Border Patrol agents noted that Block 1 offered functionality above existing technologies, it was not adequate for optimal effectiveness in detecting items of interest along the border. Users also raised concerns about the accuracy of Block 1's radar, the range of its cameras, and the quality of its video. Officials attributed some of the identified problems to users' insufficient familiarity with Block 1; however, Border Patrol officials reported that the participating agents had experience with the existing technologies and had received 2 days of training prior to the assessment. The Border Patrol thus maintained that the concerns generated should be considered operationally relevant.

Effectively managing identified defects requires a defined process for, among other things, assigning priorities to each defect and ensuring that more severe ones are given priority attention. However, the SPO does not have such a documented approach but instead relies on the prime contractor for doing so. Under this approach, defects were not consistently assigned priorities. Specifically, about 60 percent (or 801 of 1,333) of Block 1 defects identified from March 2008 to July 2009 were not assigned a priority. This is partly attributable to the SPO's lack of a defined process for

prioritizing and managing defects. Officials acknowledge this and stated that they intend to have the contractor prioritize all defects in advance of future test readiness reviews. Until defects are managed on a priority basis, the program office cannot fully understand Block 1's maturity or its exposure to related risks, nor can it make informed decisions about allocating limited resources to address defects.

DHS Science and Technology Directorate Testing Process Is Being Used to Leverage Maturing Technologies for SBI*net*

The SPO does not have its own process for testing the relevance to SBI*net* of technologies that are maturing or otherwise available from industry or other government entities. Instead, it relies on DHS's Science and Technology Directorate (S&T), whose mission is to provide technology solutions that assist DHS programs in achieving their missions. To leverage S&T, CBP signed a multiyear Interagency Agreement with the directorate in August 2007. According to this agreement, S&T is to research, develop, assess, test, and report on available and emerging technologies that could be incorporated into the SBI*net* system. To date, S&T has focused on potential technologies to fill known performance gaps or improve upon already-made technology choices, such as gaps in the radar system's ability to distinguish true radar hits from false alarms. S&T officials told us that they interact with Department of Defense (DOD) components and research entities to identify DOD systems for SBI*net* to leverage. In this regard, SPO officials stated that the current SBI*net* system makes use of DOD technologies, such as common operating picture software and radar systems. Nevertheless, S&T officials added that defense-related technologies are not always a good fit with SBI*net*, due to operational differences.

GAO Is Making Recommendations to Improve SBI*net* Test Management and Problem Resolution

To improve the planning and execution of future test events and the resolution and disclosure of system problems, we are making the following four recommendations to DHS:

- Revise the SBI*net* Test and Evaluation Master Plan to include explicit criteria for assessing the quality of test documentation and for analyzing, prioritizing, and resolving defects.

- Ensure that test schedules, plans, cases, and procedures are adequately reviewed and approved consistent with the Test and Evaluation Master Plan.

- Ensure that sufficient time is provided for reviewing and approving test documentation prior to beginning a given test event.

- Triage the full inventory of unresolved problems, including identified user concerns, and periodically report the status of the highest priority defects to Customs and Border Protection and Department of Homeland Security leadership.

In written comments on a draft of our report, DHS stated that the report was factually sound, and it agreed with our last three recommendations and agreed with all but one aspect of the first one. DHS also described actions under way or planned to address the recommendations.

In closing, I would like to stress how integral effective testing and problem resolution are to successfully acquiring and deploying a large-scale, complex system, like SBI*net* Block 1. As such, it is important that each phase of Block 1 testing be managed with rigor and discipline. To do less increases the risk that a deployed version of the system will not perform as intended, and will ultimately require costly and time-consuming rework to fix problems found later rather than sooner. Compounding this risk is the unfavorable trend in the number of unresolved system problems, and the lack of visibility into the true magnitude of these problems' severity. Given that major test events remain to be planned and conducted, which in turn are likely to identify additional system problems, it is important to correct these testing and problem resolution weaknesses.

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

Contacts and Staff Acknowledgments

For questions about this statement, please contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov. Individuals making key contributions to this testimony include Deborah Davis, Assistant Director; Carl Barden, James Crimmer, Neil Doherty, Lauren Giroux, Nancy Glover, Dan Gordon, Lee McCracken, Sushmita Srikanth, and Jennifer Stavros-Turner.

Attachment 1 – Summary of GAO's Ongoing SBI*net* Work for the Committee on Homeland Security

SBI*net's* Commitment, Progress, and Acquisition Management. Our objectives are to determine the extent to which DHS has (1) defined the scope of its proposed system solution, (2) developed a reliable schedule for delivering this solution, (3) demonstrated the cost effectiveness of this solution, (4) acquired this solution in accordance with key life cycle management processes, and (5) addressed our recent recommendations. We plan to report our results in April 2010.

SBI*net*'s Contractor Management and Oversight. Our objectives are to determine the extent to which DHS (1) has established and implemented effective controls for managing and overseeing the SBInet prime contractor and (2) is effectively monitoring the prime contractor's progress in meeting cost and schedule expectations. We plan to report our results during the summer of 2010.

Security Border Initiative Financial Management Controls Over Contractor Oversight. Our objectives are to determine the extent to which DHS has (1) developed internal control procedures over SBI*net* contractor invoice processing and contractor compliance with selected key contract terms and conditions and (2) implemented internal control procedures to ensure payments to SBI*net*'s prime contractor are proper and in compliance with selected key contract terms and conditions. We plan to report our results during the summer of 2010.

(310665)