United States Government Accountability Office

GAO

Testimony Before the Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, September 10, 2008

SECURE BORDER INITIATIVE

DHS Needs to Address Significant Risks in Delivering Key Technology Investment

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

GAO-08-1148T

September 10, 2008

SECURE BORDER INITIATIVE

DHS Needs to Address Significant Risks in Delivering Key Technology Investment

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-1148T, a testimony before the Committee on Homeland Security, House of Representatives

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 testify on its draft report, which assesses DHS's efforts to (1) define the scope, timing, and life cycle management approach for planned SBI*net* capabilities and (2) manage SBI*net* requirements and testing activities. In preparing the draft report, GAO reviewed key program documentation, including guidance, plans, and requirements and testing documentation, interviewed program officials, analyzed a random probability sample of system requirements, and observed operations of the initial SBI*net* project.

To view the full product, including the scope and methodology, click on GAO-08-1148T. 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 and when, where, and how they will be delivered. For example, the scope and timing of planned SBI*net* deployments and capabilities have continued to be delayed without becoming more specific. Further, the program office does not have an approved integrated master schedule to guide the execution of the program, and the nature and timing of planned activities 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.*

SBI*net* requirements have not been effectively defined and managed. While the program office recently issued guidance that is consistent with recognized leading practices, this guidance was not finalized until February 2008, and thus was not used in performing a number of important requirements-related activities. In the absence of this guidance, the program's efforts have been mixed. For example, while the program has taken steps to include users in developing high-level requirements, several requirements definition and management limitations exist. These include a lack of proper alignment (i.e., traceability) among the different levels of requirements, as evidenced by GAO's analysis of a random probability sample of requirements, which revealed large percentages that were not traceable backward to higher level requirements, or forward to more detailed system design specifications and verification methods.

SBI*net* testing has also not been effectively managed. 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 high-level master schedule of SBI*net* test activities, metrics for measuring testing progress, and a clear definition of testing roles and responsibilities. Further, the program office has not tested the individual system components to be deployed to the initial deployment locations, even though the contractor initiated testing of these components with other system components and subsystems in June 2008.

In light of these circumstances, our soon to be issued report contains eight recommendations to the department aimed at reassessing its approach to and plans for the program, including its associated exposure to cost, schedule and performance risks, and disclosing these risks and alternative courses of action to DHS and congressional decision makers. The recommendations also provide for correcting the weaknesses surrounding the program's unclear and constantly changing commitments and its life cycle management approach and processes, as well as implementing key requirements development and management and testing practices.

Mr. Chairman and Members of the Committee:

I appreciate the opportunity to participate in today's hearing on the Department of Homeland Security's (DHS) Secure Border Initiative (SBI). SBI is a multiyear, multibillion-dollar program to secure the nation's borders through enhanced use of surveillance technologies, increased staffing levels, improved infrastructure, and increased domestic enforcement of immigration laws. One component of SBI, known as SBI*net*, is focused on the acquisition and deployment of surveillance and command, control, communications, and intelligence technologies. This technology component is managed by the SBI*net* System Program Office within U.S. Customs and Border Protection (CBP).

My statement summarizes our draft report on the department's efforts to define the scope, timing, and life cycle management approach for planned SBI*net* capabilities, as well as its efforts to manage SBI*net* requirements and testing activities. This report is based on a review of key program-related guidance, plans, and requirements and testing documentation, as well as our analysis of a random probability sample of system requirements, and our observations of operations of the initial SBI*net* project. In comments on a draft of this report, DHS stated that the report was factually sound, and it agreed with 7 of 8 recommendations and partially disagreed with the remaining recommendation. The department also stated that it is working to address our recommendations and resolve the management and operational challenges that the report identifies as expeditiously as possible. We plan to issue our final report on September 22, 2008. Both the report and this statement are based on work that we 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 provides a reasonable basis for our findings and conclusions based on our audit objectives.

Summary

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 and when, where, 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 remain unclear. Further, the program office does not have an approved integrated master schedule to guide the execution of the program and the nature and timing of planned activities have continued to change. This schedule-related risk is exacerbated by the continuous change in, and the absence of a clear definition of, the life cycle management approach that is being used to define, develop, acquire, test, and deploy SBI*net.*

Further, SBI*net* requirements have not been effectively defined and managed. While the program office recently issued guidance that does a good job of defining key practices for effectively developing and managing requirements, the guidance was developed after several important activities had been completed. In the absence of this guidance, the program has not effectively performed key requirements definition and management practices, such as ensuring that different levels of requirements are properly aligned.

Finally, SBI*net* testing has not been effectively managed. 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 high-level master schedule of SBI*net* test activities and a clear definition of testing roles and responsibilities. Further, the program office has not tested the individual system components to be deployed to the initial deployment locations, even though the contractor initiated testing of these components with other system components and subsystems in June 2008.

Collectively, the above limitations in the scope and timing of SBI*net*'s to-be-deployed capabilities, and the ambiguity surrounding the schedule and approach for accomplishing these deployments, as well as the weaknesses in requirements development and management and in test management, introduce considerable risks to the program. As such, it is imperative that the department immediately reevaluate its plans and approach in relation to the

status of the system and related development, acquisition, and testing activities. Our soon to be issued report contains recommendations to accomplish these things. Until DHS implements them, the chances that the system will require expensive and time-consuming rework, and that it will not meet user needs and perform as intended, will increase.

Today we are also providing a statement for this committee that provides observations on SBI*net* tactical infrastructure (e.g. fencing) and the status of human capital and staffing efforts.[1]

Background

CBP's SBI program is to leverage technology, tactical infrastructure,[2] and people to allow CBP agents to gain control of the nation's borders. Within SBI, SBI*net* is the program for acquiring, developing, integrating, and deploying an appropriate mix of surveillance technologies and command, control, communications, and intelligence (C3I) technologies.

The surveillance technologies are to include a variety of sensor systems aimed at improving CBP's ability to detect, identify, classify, and track items of interest along the borders. Unattended ground sensors are to be used to detect heat and vibrations associated with foot traffic and metal associated with vehicles. Radars mounted on fixed and mobile towers are to detect movement, and cameras on fixed and mobile towers are to be used to identify, classify, and track items of interest detected by the ground sensors and the radars. Aerial assets are also to be used to provide video and infrared imaging to enhance tracking of targets.

The C3I technologies are to include software and hardware to produce a Common Operating Picture (COP)—a uniform

[1] GAO, *Secure Border Initiative: Observations on Deployment Challenges*, GAO-08-1141T (Washington, D.C.: Sept. 2008).

[2] Tactical infrastructure includes, for example, roads, vehicle barriers, and pedestrian fences.

presentation of activities within specific areas along the border. The sensors, radars, and cameras are to gather information along the border, and the system is to transmit this information to the COP terminals located in command centers and agent vehicles, assembling this information to provide CBP agents with border situational awareness.

SBI*net* Life Cycle Management Approach

A system life cycle management approach typically consists of a series of phases, milestone reviews, and related processes to guide the acquisition, development, deployment, and operation and maintenance of a system. The phases, reviews, and processes cover such important life cycle activities as requirements development and management, design, software development, and testing.

In general, SBI*net s*urveillance systems are to be acquired through the purchase of commercially available products, while the COP systems involve development of new, customized systems and software. Together, both categories are to form a deployable increment of SBI*net* capabilities, which the program office refers to as a "block." Each block is to include a release or version of the COP. The border area that receives a given block is referred to as a "project."

Among the key processes provided for in the SBI*net* system life cycle management approach are processes for developing and managing requirements and for managing testing activities. SBI*net* requirements are to consist of a hierarchy of six types of requirements, with the high-level operational requirements at the top. These high-level requirements are to be decomposed into lower-level, more detailed system, component, design, software, and project requirements. SBI*net* testing consists of a sequence of tests that are intended to first verify that individual system parts meet specified requirements, and then verify that these combined parts perform as intended as an integrated and operational system. Having a decomposed hierarchy of requirements and an incremental approach to testing are both characteristics of complex information technology (IT) projects.

Limited Definition of SBI*net* Deployments, Capabilities, Schedule, and Lifecycle Management Process Increases Program's Exposure to Risk

Important aspects of SBI*net*—the scope, schedule, and development and deployment approach—remain ambiguous and in a continued state of flux, making it unclear and uncertain what technology capabilities will be delivered and when, where, 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 remain unclear. Further, the approach that is being used to define, develop, acquire, test, and deploy SBI*net* is similarly unclear and has continued to change. The absence of clarity and stability in these key aspects of SBI*net* introduces considerable program risks, hampers DHS's ability to measure program progress, and impairs the ability of Congress to oversee the program and hold DHS accountable for program results.

Scope and Timing of Planned Deployments and Capabilities Are Not Clear and Stable

The scope and timing of planned SBI*net* deployments and capabilities have not been clearly established, but rather have continued to change since the program began. Specifically, as of December 2006, the SBI*net* System Program Office planned to deploy an "initial" set of capabilities along the entire southwest border by late 2008 and a "full" set of operational capabilities along the southern and northern borders (a total of about 6,000 miles) by late 2009.

Since then, however, the program office has modified its plans multiple times. As of March 2008, it planned to deploy SBI*net* capabilities to just three out of nine sectors along the southwest border: Tucson Sector by 2009, Yuma Sector by 2010, and El Paso Sector by 2011. According to program officials, no deployment dates had been established for the remainder of the southwest or northern borders.

At the same time, the SBI*net* System Program Office committed to deploying Block 1 technologies to two locations within the Tucson

sector by the end of 2008, known as Tucson 1 and Ajo 1. However, as of late July 2008, program officials reported that the deployment schedule for these two sites has been modified, and they will not be operational until "sometime" in 2009. The slippages in the dates for the first two Tucson deployments, according to a program official, will, in turn, delay subsequent Tucson deployments, although revised dates for these subsequent deployments have not been set.

In addition, the current Block 1 design does not provide key capabilities that are in requirements documents and were anticipated to be part of the Block 1 deployments to Tucson 1 and Ajo 1. For example, the first deployments of Block 1 will not be capable of providing COP information to the agent vehicles. Without clearly establishing program commitments, such as capabilities to be deployed and when and where they are to be deployed, program progress cannot be measured and responsible parties cannot be held accountable.

Program Schedule Is Unsettled

Another key aspect of successfully managing large programs like SBI*net* is having a schedule that defines the sequence and timing of key activities and events and is realistic, achievable, and minimizes program risks. However, the timing and sequencing of the work, activities, and events that need to occur to meet existing program commitments are also unclear. Specifically, the program office does not yet have an approved integrated master schedule to guide the execution of SBI*net*. Moreover, our assimilation of available information from multiple program sources indicates that the schedule has continued to change. Program officials attributed these schedule changes to the lack of a satisfactory system-level design, turnover in the contractor's workforce, including three different program managers and three different lead system engineers, and attrition in the SBI*net* Program Office, including turnover in the SBI*net* Program Manager position. Without stability and certainty in the program's schedule, program cost and schedule risks increase, and meaningful measurement and oversight of program status and progress cannot occur, in turn limiting accountability for results.

SBI*net* Life Cycle Management Approach Has Not Been Clearly Defined and Has Continued to Change

System quality and performance are in large part governed by the approach and processes followed in developing and acquiring the system. The approach and processes should be fully documented so that they can be understood and properly implemented by those responsible for doing so, thus increasing the chances of delivering promised system capabilities and benefits on time and within budget.

The life cycle management approach and processes being used by the SBI*net* System Program Office to manage the definition, design, development, testing, and deployment of system capabilities has not been fully and clearly documented. Rather, what is defined in various program documents is limited and not fully consistent across these documents. For example, officials have stated that they are using the draft Systems Engineering Plan, dated February 2008, to guide the design, development, and deployment of system capabilities, and the draft Test and Evaluation Master Plan, dated May 2008, to guide the testing process, but both of these documents appear to lack sufficient information to clearly guide system activities. For example, the Systems Engineering Plan includes a diagram of the engineering process, but the steps of the process and the gate reviews are not defined or described in the text of the document. Further, statements by program officials responsible for system development and testing activities, as well as briefing materials and diagrams that these officials provided, did not add sufficient clarity to describe a well-defined life cycle management approach.

Program officials told us that both the government and contractor staff understand the SBI*net* life cycle management approach and related engineering processes through the combination of the draft Systems Engineering Plan and government/contractor interactions during design meetings. Nevertheless, they acknowledged that the approach and processes are not well documented, citing a lack of sufficient staff to both document the processes and oversee the system's design, development, testing, and deployment. They also told us that they are adding new people to the program office with

different acquisition backgrounds, and they are still learning about, evolving, and improving the approach and processes. The lack of definition and stability in the approach and related processes being used to define, design, develop, acquire, test, and deploy SBI*net* introduces considerable risk that both the program officials and contractor staff will not understand what needs to be done when, and that the system will not meet operational needs and perform as intended.

Limitations of SBI*net* Requirements Development and Management Efforts Increase Program Risk

DHS has not effectively defined and managed SBI*net* requirements. While the program office recently issued guidance that is consistent with recognized leading practices,[3] this guidance was not finalized until February 2008, and thus was not used in performing a number of key requirements-related activities. In the absence of well-defined guidance, the program's efforts to effectively define and manage requirements have been mixed. For example, the program has taken credible steps to include users in the definition of requirements. However, several requirements definition and management limitations exist.

Program Office Has Taken Steps to Involve Users in Developing High-level Requirements

One of the leading practices associated with effective requirements development and management is engaging system users early and continuously. In developing the operational requirements, the System Program Office involved SBI*net* users in a manner consistent with leading practices. Specifically, it conducted requirements-gathering workshops from October 2006 through April

[3]The Capability Maturity Model Integration for Development® developed by the Software Institute of Carnegie Mellon University defines key practices that are recognized hallmarks for successful organizations that, if effectively implemented, can greatly increase the chances of successfully developing and acquiring software and systems. See Carnegie Mellon Software Engineering Institute, Capability Maturity Model Integration for Development® version 1.2 (Pittsburgh, Penn., August 2006*).*

2007 to ascertain the needs of Border Patrol agents and established work groups in September 2007 to solicit input from both the Office of Air and Marine Operations and the Office of Field Operations. Further, the program office is developing the COP technology in a way that allows end users to be directly involved in software development activities, which permits solutions to be tailored to their needs.[4] Such efforts increase the chances of developing a system that will successfully meet those needs.

Not All Levels of Requirements Have Been Adequately Baselined

The creation of a requirements baseline establishes a set of requirements that have been formally reviewed and agreed on, and thus serve as the basis for further development or delivery. According to SBI*net* program officials, the SBI*net* Requirements Development and Management Plan, and leading practices, requirements should be baselined before key system design activities begin in order to inform, guide, and constrain the system's design.

While many SBI*net* requirements have been baselined, two types have not yet been baselined. According to the System Program Office, the operational requirements, system requirements, and various system component requirements have been baselined. However, as of July 2008, the program office had not baselined its COP software requirements and its project-level requirements for the Tucson sector, which includes Tucson 1 and Ajo 1. According to program officials the COP requirements have not been baselined because certain interface requirements[5] had not yet been completely identified and defined. Despite the absence of baselined COP and project-level requirements, the program office has proceeded with development, integration, and testing activities for the Block 1 capabilities to be delivered to Tucson 1 and Ajo l. As a result, it

[4]This method, Rapid Application Development and Joint Application Design (RAD/JAD), uses graphical user interfaces and direct end user involvement in a collaborative development approach.

[5] Interface requirements describe the capabilities which must be in place in order to integrate components and products together.

faces increased risks of deploying systems that do not align well with requirements, and thus will require subsequent rework.

SBI*net* Requirements Have Not Been Sufficiently Aligned

Another leading practice associated with developing and managing requirements is maintaining bidirectional traceability from high-level operational requirements through detailed low-level requirements to test cases. The SBI*net* Requirements Development and Management Plan recognizes the importance of traceability, and the SBI*net* System Program Office established detailed guidance[6] for populating and maintaining a requirements database for maintaining linkages among requirement levels and test verification methods.

To provide for requirements traceability, the prime contractor established such a requirements management database. However, the reliability of the database is questionable. We attempted to trace requirements in the version of this database that the program office received in March 2008, and were unable to trace large percentages of component requirements to either higher-level or lower level requirements. For example, an estimated 76 percent (with a 95 percent degree of confidence of being between 64 and 86 percent) of the component requirements that we randomly sampled could not be traced to the system requirements and then to the operational requirements. In addition, an estimated 20 percent (with a 95 percent degree of confidence of being between 11 and 33 percent) of the component requirements in our sample failed to trace to a verification method. Without ensuring that requirements are fully traceable, the program office does not have a sufficient basis for knowing that the scope of the contractor's design, development, and testing efforts will produce a system solution that meets operational needs and performs as intended.

[6]SBI*net* Requirements Management Plan, January 15, 2007.

Limitations in Key SBI*net* Testing and Test Management Activities Increase Program Risk

To be effectively managed, testing should be planned and conducted in a structured and disciplined fashion. This includes having an overarching test plan or strategy and testing individual system components to ensure that they satisfy requirements prior to integrating them into the overall system. This test management plan should define the schedule of high-level test activities in sufficient detail to allow for more detailed test planning and execution to occur, define metrics to track test progress and report and address results, and define the roles and responsibilities of the various groups responsible for different levels of testing.

However, the SBI*net* program office is not effectively managing its testing activities. Specifically, the SBI*net* Test and Evaluation Master Plan, which documents the program's test strategy and is being used to manage system testing, has yet to be approved by the SBI*net* Acting Program Manager, even though testing activities began in June 2008. Moreover, the plan is not complete. In particular, it does not (1) contain an accurate and up-to-date test schedule, (2) identify any metrics for measuring testing progress, and (3) clearly define and completely describe the roles and responsibilities of various entities that are involved in system testing.

Further, the SBI*net* System Program Office has not performed individual component testing as part of integration testing. As of July 2008, agency officials reported that component-level tests had not been completed and were not scheduled to occur. Instead, officials stated that Block 1 components were evaluated based on what they described as "informal tests" (i.e., contractor observations of cameras and radar suites in operation at a National Guard facility in the Tucson sector), and that the contractors' self-certification that the components meet functional and performance requirements was acceptable. Program officials acknowledged that this approach did not verify whether the individual components in fact met requirements.

Without effectively managing testing activities, the chances of SBI*net* testing being effectively performed is reduced, which in turn increases the risk that the delivered and deployed system will not meet operational needs and not perform as intended.

In closing, I would like to stress that a fundamental aspect of successfully implementing a large IT program like SBI*net* is establishing program commitments, including what capabilities will be delivered and when and where they will be delivered. Only through establishing such commitments, and adequately defining the approach and processes to be used in delivering them, can DHS effectively position itself for measuring progress, ensuring accountability for results, and delivering a system solution with its promised capabilities and benefits on time and within budget constraints. For SBI*net*, this has not occurred to the extent that it needs to for the program to have a meaningful chance of succeeding. In particular, commitments to the timing and scope of system capabilities remain unclear and continue to change, with the program committing to far fewer capabilities than originally envisioned. Further, how the SBI*net* system solution is to be delivered has been equally unclear and inadequately defined. Moreover, while the program office has defined key practices for developing and managing requirements, these practices were developed after several important requirements activities were performed. In addition, efforts performed to date to test whether the system meets requirements and functions as intended have been limited.

Collectively, these limitations increase the risk that the delivered system solution will not meet user needs and operational requirements and will not perform as intended. In turn, the chances are increased that the system will require expensive and time-consuming rework. In light of these circumstances and risks surrounding SBI*net*, our soon to be issued report contains eight recommendations to the department aimed at reassessing its approach to and plans for the program, including its associated exposure to cost, schedule, and performance risks, and disclosing these risks and alternative courses of action for addressing them to DHS and congressional decision makers. The recommendations also

provide for correcting the weaknesses surrounding the program's unclear and constantly changing commitments and its life cycle management approach and processes, as well as implementing key requirements development and management and testing practices.

While implementing these recommendations will not guarantee a successful program, it will minimize the program's exposure to risk and thus the likelihood that it will fall short of expectations. For SBI*net*, living up to expectations is important because the program is a large, complex, and integral component of DHS's border security and immigration control strategy.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the committee may have at this time.

Contacts and Acknowledgements

For further information, please contact Randolph C. Hite at (202) 512-3439 or by email at hiter@gao.gov. Other key contributors to this testimony were Carl Barden, Deborah Davis, Neil Doherty, Lee McCracken, Jamelyn Payan, Karl Seifert, Sushmita Srikanth, Karen Talley, and Merry Woo.

(310667)