

September 2008

SECURE BORDER INITIATIVE

DHS Needs to Address Significant Risks in Delivering Key Technology Investment





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.

SECURE BORDER INITIATIVE

DHS Needs to Address Significant Risks in Delivering Key Technology Investment

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.

Contents

Letter		1
	Results in Brief	2
	Background	6
	Limited Definition of <i>SBI</i> net Deployments, Capabilities, Schedule, and Life Cycle Management Process Increases Program's Exposure to Risk	16
	Limitations of <i>SBI</i> net Requirements Development and Management Efforts Increase Program Risk	24
	Limitations in Key <i>SBI</i> net Testing and Test Management Activities Increase Program Risk	32
	Conclusions	37
	Recommendations for Executive Action	38
	Agency Comments and Our Evaluation	39
Appendix I	Objectives, Scope, and Methodology	42
Appendix II	Comments from the Department of Homeland Security	45
Appendix III	GAO Contact and Staff Acknowledgments	51
Tables		
	Table 1: System-Level Reviews and Their Purpose	12
	Table 2: Project-Level Reviews and Their Purpose	13
	Table 3: <i>SBI</i> net Requirements Types	14
	Table 4: <i>SBI</i> net Tests	15
	Table 5: <i>SBI</i> net Requirements Traceability Results	31
	Table 6: Roles and Responsibilities of Entities Identified in the Draft <i>SBI</i> net Test and Evaluation Master Plan	36
Figures		
	Figure 1: High-Level, Conceptual Depiction of Long-Term <i>SBI</i> net Operations	7
	Figure 2: COP in a Command Center and Agent Vehicle	9

Figure 3: SBI <i>net</i> Building Block Approach	11
Figure 4: Relationships among Requirements	14
Figure 5: Changes in Planned Deployments over Time	17
Figure 6: Changes in Schedules for Reviews and Deployment	20
Figure 7: Changes in Schedules for Testing	21

Abbreviations

CBP	U.S. Customs and Border Protection
CDR	Critical Design Review
COP	Common Operating Picture
C3I	command, control, communications and intelligence
DDR	Deployment Design Review
DHS	Department of Homeland Security
DOORS	Dynamic Object-Oriented Requirements System
DRR	Deployment Readiness Review
IT	information technology
PDR	Preliminary Design Review
RAD/JAD	Rapid Application Development and Joint Application Design
SBI	Secure Border Initiative
SRR	System Requirements Review
TRR	Test Readiness Review

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

September 22, 2008

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

The Honorable Christopher P. Carney
Chairman
The Honorable Mike Rogers
Ranking Member
Subcommittee on Management, Investigations, and Oversight
Committee on Homeland Security
House of Representatives

The Honorable Kendrick B. Meek
House of Representatives

Securing the nation's borders from illegal entry of aliens and contraband continues to be a major challenge because much of the 6,000 miles¹ of international borders with Canada and Mexico remains vulnerable to unlawful activities. Although the Department of Homeland Security (DHS) apprehends hundreds of thousands of people entering the country illegally each year, many more unauthorized entrants go undetected.

As we have reported, previous attempts to acquire and deploy surveillance technologies along the nation's borders to assist in detecting and responding to illegal entries have not been successful. Specifically, the former Immigration and Naturalization Service's Integrated Surveillance Intelligence System, begun in the late 1990s, was difficult and expensive to maintain; it provided limited command, control, and situational awareness capability; and its component systems were not integrated.² In response, DHS established the America's Shield Initiative in 2004, but this program was halted in 2005 because of the program's limited scope and the department's shift in strategy for achieving border security and interior

¹The scope of *SBI*net is the contiguous United States' land border with Mexico and Canada.

²GAO, *Border Security: Key Unresolved Issues Justify Reevaluation of Border Surveillance Technology Program*, [GAO-06-295](#) (Washington, D.C.: Feb. 22, 2006).

enforcement goals.³ In November 2005, DHS launched the Secure Border Initiative (SBI), 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 communications technologies. This program is managed by the *SBI_{net}* System Program Office within U.S. Customs and Border Protection (CBP).

Because of the size and complexity of *SBI_{net}*, and the problems experienced by its predecessors, you asked us to determine whether DHS (1) has defined the scope and timing of planned *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 accomplish our objectives, we reviewed key program documentation, including guidance, plans, and requirements and testing documentation. In cases where such documentation was not available, we interviewed program officials about the development of capabilities and the management of requirements and testing. We then compared this information to relevant federal system acquisition guidance. We also analyzed a random probability sample of system requirements and observed operations of the initial *SBI_{net}* project.

We conducted this performance audit from August 2007 to September 2008 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. Further details of our objectives, scope, and methodology are included in appendix I.

Results in Brief

Important aspects of *SBI_{net}*—the scope and schedule, and the development and deployment approach—remain ambiguous and in a continued state of flux, making it unclear and uncertain what technology

³[GAO-06-295](#).

capabilities will be delivered, when and where they will be delivered, and how they will be delivered, as the following examples illustrate:

- The scope of what is to be achieved has become more limited without becoming more specific. In particular, in December 2006, the department committed to having an initial set of capabilities operational along the entire southwest border by late 2008 and having a full set of capabilities operational along the entire southwest and northern borders by late 2009. In March 2008, the *SBI*net System Program Office had reduced its commitment to deploying a to-be-determined set of technology capabilities to three out of nine sectors⁴ along the southwest border by 2011 and to only two locations in one of nine sectors by the end of 2008. As of July 2008, the program office reported that the dates for the two locations would slip into 2009; however, specific dates were not available and thus remain uncertain.
- The timing and sequencing of the work, activities, and events that need to occur have continued to be unclear. Specifically, the program office does not have an approved integrated master schedule to govern the execution of the program. Further, our assimilation of available information from multiple program sources indicates that the schedule has continued to change.
- This schedule-related risk is exacerbated by the continuous change in and absence of clear definition around the system life cycle management approach that is being used to develop and deploy *SBI*net. In particular, important details about key life cycle processes are not documented, and what is defined in various documents is not fully consistent across them. Moreover, in discussions with agency officials to obtain clarification regarding the processes, new information has been introduced routinely, as recently as late July 2008, which differs from available documentation or earlier statements by these officials.

*SBI*net requirements have not been effectively developed 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, documenting and approving

⁴CBP divides the United States' borders with Mexico and Canada into 20 sectors responsible for detecting, interdicting, and apprehending those who attempt illegal entry or to smuggle contraband across U.S. borders.

the requirements to establish a baseline,⁵ and ensuring that requirements are traceable—the guidance was not used in developing *SBI_{net}* requirements because it was issued after their development. 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 development and management limitations exist. For example, all requirements have not been finalized, such as the requirements for the command, control, and communication subsystem of *SBI_{net}* and the requirements specific to the first two deployment locations. Also, an independent review found some of the operational requirements to be unverifiable or unaffordable, indicating that these requirements had not been properly defined and validated. Moreover, the different levels of requirements are not properly aligned (i.e., traceable), as evidenced by our analysis of a random probability sample of requirements where we found large percentages that were not traceable back to higher level requirements or forward to more detailed system design specifications and verification methods.

SBI_{net} testing has not been effectively managed. Specifically, critical testing activities, as called for in federal guidance⁶ and described in the program office’s own test documents, have yet to be performed, and the infrastructure for managing testing has not been fully established. For example, the program office has not tested the individual system components to be deployed to the initial two locations, even though the contractor initiated integration testing of multiple components with the command, control, and communication subsystem in June 2008. Further, while a test management strategy, known as the Test and Evaluation Master Plan, was drafted in May 2008, it has not been finalized and approved, and it does not contain, among other things, clear definitions 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.

⁵Carnegie Mellon Software Engineering Institute’s Capability Maturity Model® Integration for Development defines a baseline as a set of specifications or work products that has been formally reviewed and agreed on, which thereafter serves as the basis for further development or delivery, and that can be changed only through change control procedures.

⁶See, for example, GAO, *Year 2000 Computing Crisis: A Testing Guide*, GAO/AIMD-10.1.21 (Washington, D.C.: November 1998).

Collectively, the above limitations in the scope and timing of *SBI*net to-be-deployed capabilities, the ambiguity surrounding the schedule and approach for accomplishing these deployments, and the weaknesses in requirements development and management and test management, introduce considerable risks to the program. To address these risks, we are making recommendations to DHS to immediately re-evaluate its plans and approach in relation to the status of the system and related development, acquisition, and testing activities, as discussed in this report, and to disclose to CBP and DHS leadership, as well as appropriate congressional committees, the results of this assessment, including proposed changes to its planned schedule of activities to mitigate the associated risks. In addition, we are making recommendations to address each of the system acquisition and development problems discussed in this report, including those associated with finalizing an integrated master schedule, having a well-defined and stable life cycle management approach, and implementing effective requirements development and management and testing.

In comments on a draft of this report, reprinted in appendix II, the department stated that the report was factually sound and that it agreed with seven of our eight recommendations and partially disagreed with one aspect of the remaining recommendation. Specifically, DHS disagreed with that aspect of one recommendation for conducting appropriate component-level testing prior to integrating system components, stating that its current test strategy provides the appropriate degree of confidence in these commercially available components, as evidenced by either component manufacturer certificates of conformance, independent government laboratory test documentation, or the prime contractor's component-integration level testing. We support DHS's current test strategy as it is consistent with our recommendation. Specifically, it expands on the department's prior strategy for component testing, which was limited to manufacturer self-certification of component conformance and informal observations of system components, by adding the use of independent government laboratories to test the components. We would emphasize, however, that regardless of the method used, it is important that confidence be gained in components prior to integrating them, which our recommendation recognizes. As our report states, such a hierarchical approach to testing allows for the source of any system defects to be discovered and isolated sooner rather than later, and thus helps to avoid the potential for expensive and time-consuming system rework. With respect to all of our recommendations, the department added that it is working to address our recommendations and resolve the management and operational challenges identified in the report as expeditiously as

possible, and it described actions recently completed, underway, and planned that it said would address them. The department also provided technical comments that we incorporated in the report, as appropriate.

Background

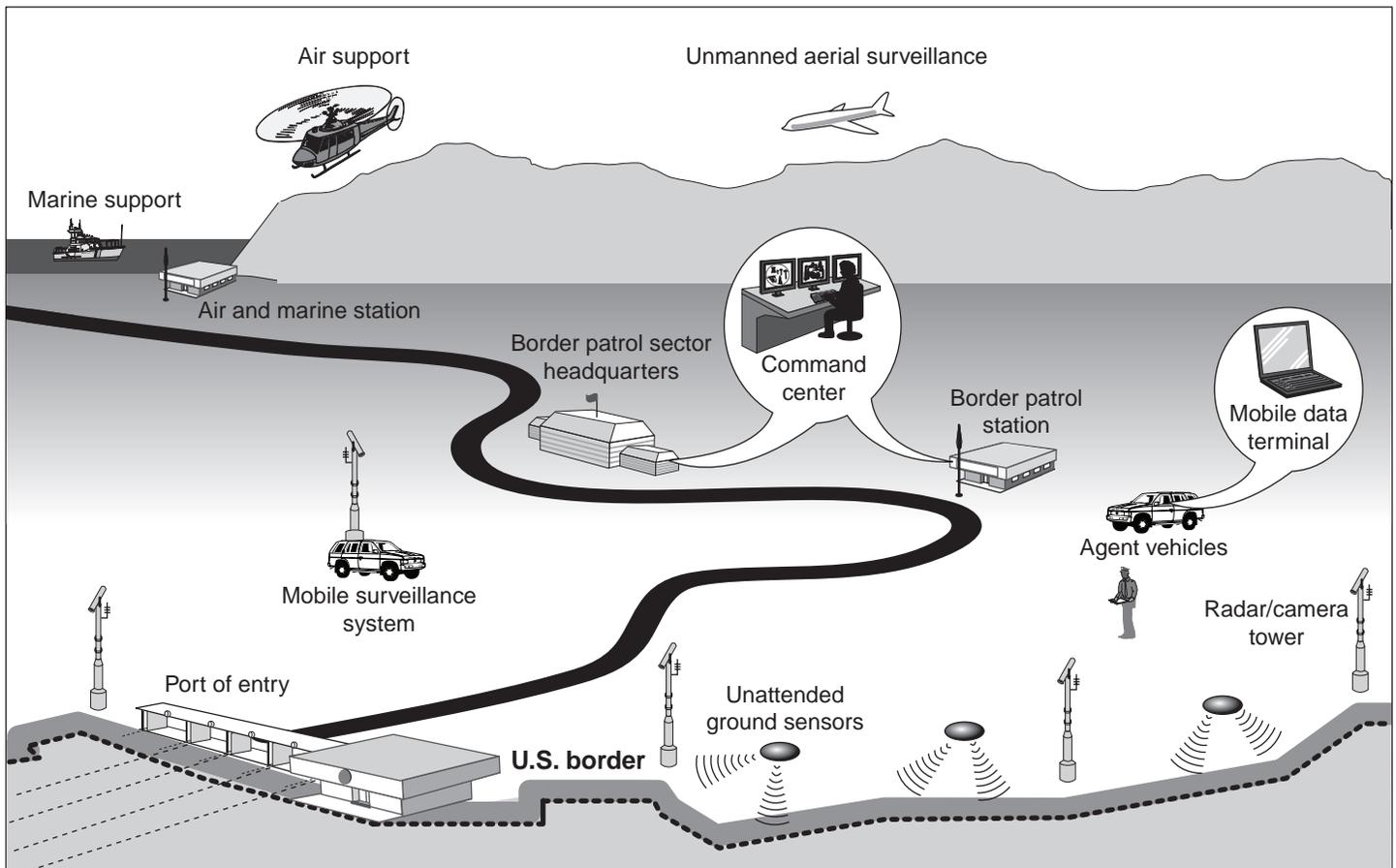
CBP's SBI program is to leverage technology, tactical infrastructure,⁷ and people to allow CBP agents to gain control of the nation's borders. Within SBI, *SBI_{net}* is the program for acquiring, developing, integrating, and deploying an appropriate mix of (1) surveillance technologies, such as cameras, radars, and sensors, and (2) command, control, communications, and intelligence (C3I) technologies.

The initial focus of *SBI_{net}* has been on addressing the requirements of CBP's Office of Border Patrol, which is responsible for securing the borders between the established ports of entry.⁸ The longer-term *SBI_{net}* systems solution also is to address requirements of CBP's two other major components—the Office of Field Operations, which controls vehicle and pedestrian traffic at the ports of entry, and the Office of Air and Marine Operations, which operates helicopters, fixed-wing aircraft, and marine vessels used in securing the borders. Figure 1 provides a high-level, operational concept of the long-term *SBI_{net}* systems solution.

⁷Tactical infrastructure includes roads, vehicle barriers, pedestrian fences, etc.

⁸At a port of entry location, CBP officers secure the flow of people and cargo into and out of the country, while facilitating legitimate travel and trade.

Figure 1: High-Level, Conceptual Depiction of Long-Term SBInet Operations



Sources: GAO analysis of agency data, Art Explosion (clip art).

Surveillance technologies are to include a variety of sensor systems that improve 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.

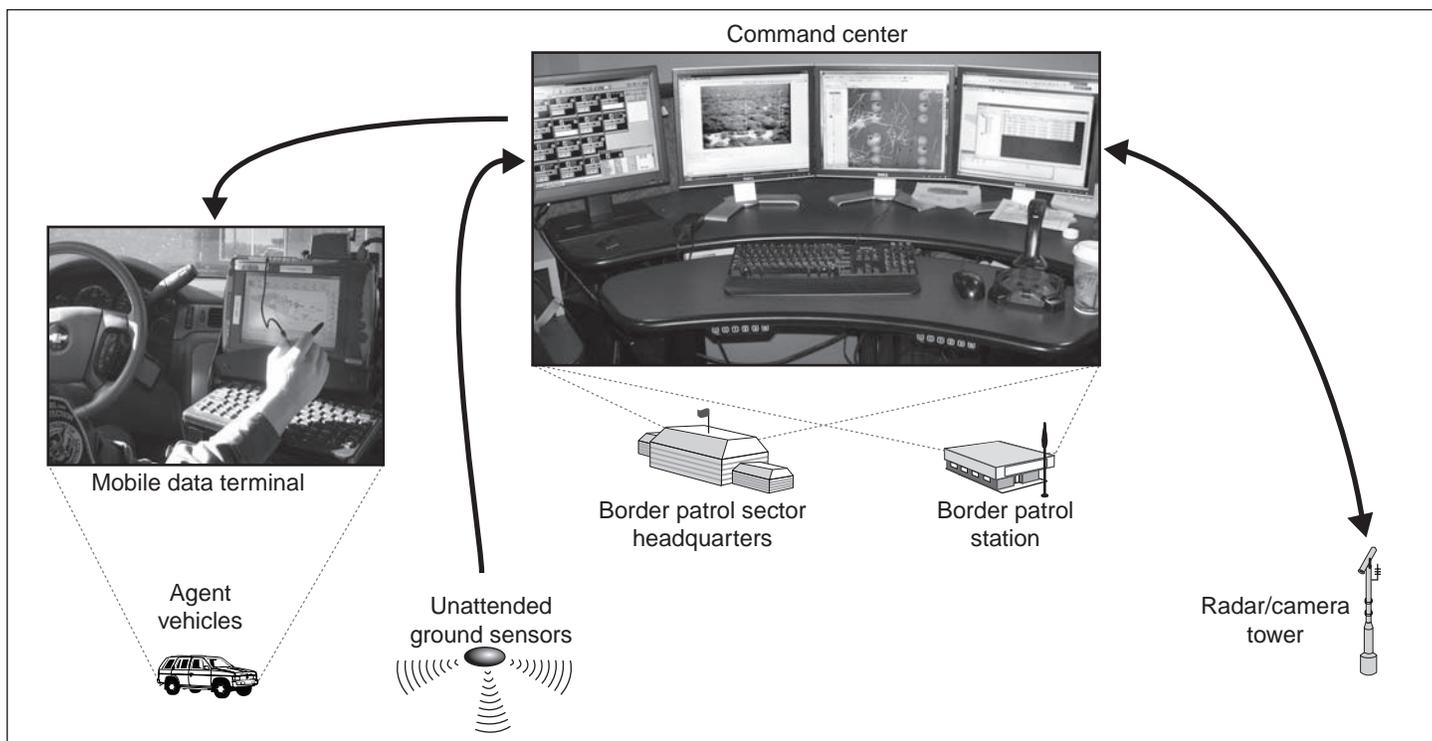
The C3I technologies are to include software and hardware to produce a Common Operating Picture (COP)—a uniform presentation of activities

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 and assemble this information to provide CBP agents with border situational awareness. More specifically, the COP technology is to allow agents to (1) view data from radars and sensors that detect and track movement in the border areas, (2) control cameras to help identify and classify illegal entries, (3) correlate entries with the positions of nearby agents, and (4) enhance tactical decision making regarding the appropriate response to apprehend an entry, if necessary.

Initially, COP information is to be distributed to terminals in command centers. We observed that these terminals look like a standard computer workstation with multiple screens. From this workstation, an operator is to be able to view an area of interest in several different ways. For example, the operator is to see different types of maps, satellite images, and camera footage on the multiple screens. The operator is also to be able to move the cameras to track images on the screen. According to program officials, eventually, when the radars detect potential items of interest, the system is to automatically move the cameras so the operator does not always need to initiate the search in the area.

We observed that COP data are also available on laptop computers, known as mobile data terminals, mounted in select agent vehicles in the field. These terminals are to enable field agents to see information similar to that seen by command center operators. Eventually, the COP technology is to be capable of providing distributed surveillance and tactical decision-support information to other DHS agencies and stakeholders external to DHS, such as local law enforcement. Figure 2 shows examples of COP technology in a command station and an agent vehicle.

Figure 2: COP in a Command Center and Agent Vehicle



Sources: GAO analysis of agency data, GAO (photos), Art Explosion (clip art).

The first *SBI*net capabilities were deployed under a pilot or prototype effort known as “Project 28.” Project 28 is currently operating along 28 miles of the southwest border in the Tucson Sector of Arizona. Project 28 was accepted by the government for deployment 8 months behind schedule (in February 2008); this delay occurred because the contractor-delivered system did not perform as intended. As we have previously reported,⁹ reasons for Project 28 performance shortfalls and delays include the following:

- System requirements were not adequately defined, and users were not involved in developing the requirements.

⁹GAO, *Secure Border Initiative: Observations on Selected Aspects of SBI*net Program Implementation, [GAO-08-131T](#) (Washington, D.C.: Oct. 24, 2007) and GAO, *Secure Border Initiative: Observations on the Importance of Applying Lessons Learned to Future Projects*, [GAO-08-508T](#) (Washington, D.C.: Feb. 27, 2008).

-
- System integration testing was not adequately performed.
 - Contractor oversight was limited.
 - Project scope and complexity were underestimated.

To manage *SBI*net, DHS established a program office within CBP. The program office is led by a program manager and deputy program managers for program operations and mission operations. The program manager is responsible for the execution of the program, including developing, producing, deploying, and sustaining the system to meet the users' needs. Among other things, this includes developing and analyzing requirements and system alternatives, managing system design and development, evaluating the system's operational effectiveness, and managing program risk.

*SBI*net Program Office Description of Its 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. Among other things, the phases, reviews, and processes cover such important life cycle activities as requirements development and management, design, software development, and testing. Based on available program documentation, augmented by program official briefings and statements, key aspects of the *SBI*net system life cycle management approach are described below.

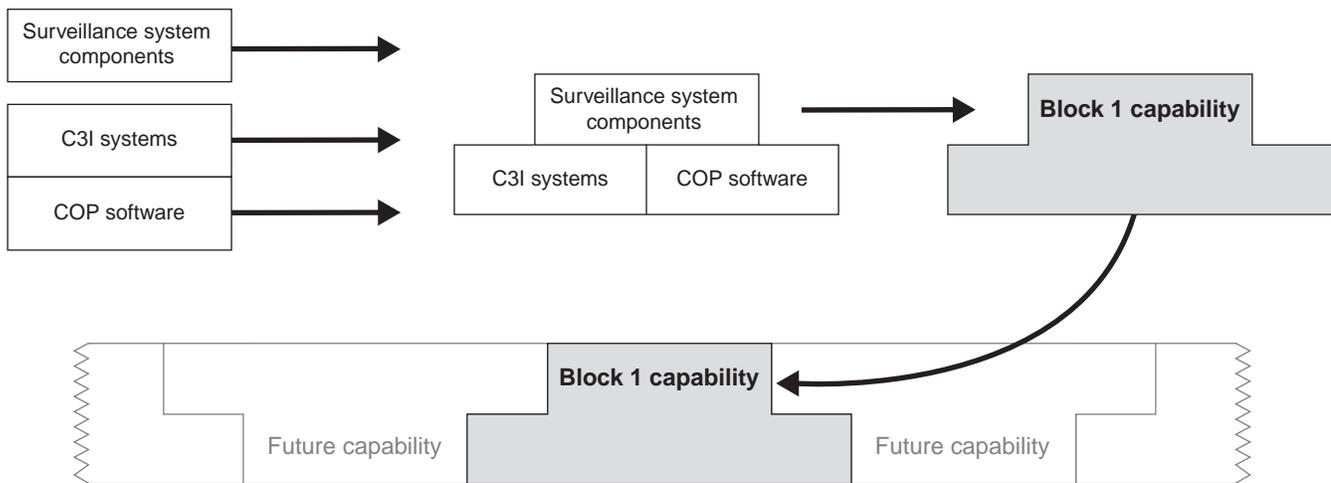
Approach Is Intended to Deliver Incremental Capabilities through a Series of Blocks

In general, *SBI*net surveillance 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 the *SBI*net capabilities, which the program office refers to as a "block." Each block is to include a release or version of the COP.

*SBI*net documentation shows that the program office is acquiring the blocks incrementally using a "spiral" approach, under which an initial system capability is to be delivered based on a defined subset of the system's total requirements. This approach is intended to allow CBP agents access to new technological tools sooner rather than later for both operational use and feedback on needed enhancements or changes. Subsequent spirals or iterations of system capability are to be delivered based on feedback and unmet requirements, as well as the availability of new technologies. Figure 3 illustrates conceptually how the different

capabilities are to come together to form a block and how future blocks are to introduce more capabilities.

Figure 3: SBInet Building Block Approach



Source: GAO analysis of agency data from multiple sources.

The approach used to design and develop SBInet system capabilities for each block includes such key activities as requirements development, system design, system acquisition and development, and testing. The approach, as explained by program officials and depicted in part in various documents, also includes various reviews, or decision points, to help ensure that these activities are being done properly and that the system meets user needs and requirements. These reviews are to be used in developing both the overall SBInet Block 1 capability and the COP software. Table 1 provides a high-level description of the major reviews that are to be performed in designing and developing the system prior to deployment to the field and in the order that they occur.¹⁰

¹⁰The list of reviews is from the draft SBInet Systems Engineering Plan, dated February 12, 2008. The actual descriptions of the reviews are from other SBInet documents.

Table 1: System-Level Reviews and Their Purpose

Review	Purpose
System Requirements Review	Ensures that system requirements have been completely and properly identified and that a mutual understanding exists between the DHS CBP <i>SBI</i> net System Program Office and the contractor on the requirements to be met.
Preliminary Design Review	Confirms that sufficient design has been accomplished to verify the completeness and achievability of system requirements.
Critical Design Review	Demonstrates that the detailed designs are complete; meet requirements; provide for external interfaces; and are ready for fabrication, coding, assembly, and integration.
System Qualification Test Readiness Review	Ensures that the test objectives are clear and test procedures are adequate to test that the system requirements are being met.
System Production Readiness Review	Demonstrates stakeholder concurrence that the system is ready for deployment and examines the program to determine if the design is ready for production.

Source: GAO analysis of *SBI*net and CBP documents.

Before a set of capabilities (i.e., block) is deployed to a specific area or sector of the border, activities such as site selection, surveys, and environmental impact assessments are conducted to determine the area's unique environmental requirements. The border area that receives a given block, or set of system capabilities, is referred to as a "project." Each project is to have a given block configured to its unique environmental requirements, referred to as a project "laydown."

The deployment approach is to include such key activities as requirements development, system design, project laydown, integration, testing, and installation. The deployment approach is also to entail various reviews, or decision points, to help ensure that these activities are being done properly and that the system meets user needs and requirements. Table 2 provides a high-level description of the major reviews that are to be part of project laydown in the order that they occur.¹¹

¹¹The list of reviews is from the draft *SBI*net Systems Engineering Plan, dated February 12, 2008. The actual descriptions of the reviews are from other *SBI*net documents.

Table 2: Project-Level Reviews and Their Purpose

Review	Purpose
Project Requirements Review ^a	Demonstrates contractor understanding and analysis of the project-level requirements.
Deployment Design Review	Ensures that the SBInet System Program Office and the contractor concur that the proposed system design meets the project-level requirements.
Deployment Readiness Review	Provides an assessment of the design maturity and ensures that the contractor is ready to begin construction, such as site preparation, building the access roads, laying the tower foundations, and installing the tower power supplies.
System Acceptance Test Readiness Review	Ensures that the test objectives are clear and test procedures are adequate to test whether or not the system is ready to be accepted by the government.
Operational Test Readiness Review	Ensures that the system can proceed to operational testing with a high probability of success.
Operational Readiness Review	Documents stakeholder concurrence that the system is ready for full operation.

Source: GAO analysis of SBInet and CBP documents.

^aCurrently referred to by the program office as "Deployment Planning Review."

Approach Includes Key Processes for Developing and Managing Requirements and for Managing Testing

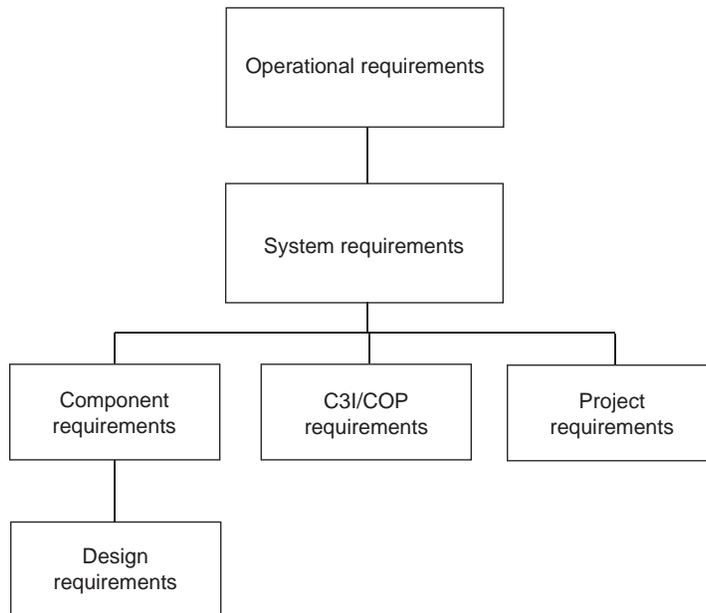
Among the key processes provided for in the SBInet system life cycle management approach are processes for developing and managing requirements and for managing testing activities. With respect to requirements development and management, SBInet requirements are to consist of a hierarchy of six types 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. Having a decomposed hierarchy of requirements is a characteristic of complex information technology (IT) projects. The various types of SBInet requirements are described in table 3. Figure 4 shows how each of these requirements relate to or are derived from the other requirements.

Table 3: SBInet Requirements Types

Type	Description
Operational requirements	Describe the missions and operational capabilities that the resulting system must satisfy. These are the user requirements for the SBInet system.
System requirements	Describe the SBInet performance and system functional and nonfunctional characteristics. Used for the design, development, integration, verification, and deployment of the SBInet system.
Component requirements	Describe required features of various surveillance components, such as cameras and radars, sufficient to guide system design. Also associated with one or more verification (test) methods that will be used to ensure that the system is in compliance with component requirements.
Design requirements	Describe the performance, design, and acceptance features for various component products, such as a short-range or long-range camera.
COP software requirements	Describe the functionality and capability of the COP software, such as allowing the user to control and view information from the sensors.
Project requirements	Describe the unique environmental requirements and capabilities that are deployed for a project (geographic area).

Source: GAO analysis of SBInet documents.

Figure 4: Relationships among Requirements



Source: DHS.

With respect to test management, *SBI_{net}* testing consists of a sequence of tests that are intended to verify first that individual system parts meet specified requirements, and then verify that these combined parts perform as intended as an integrated and operational system. Such an incremental approach to testing is a characteristic of complex IT system acquisition and development efforts. Through such an approach, the source of defects can be isolated more easily and sooner, before they are more difficult and expensive to address. Table 4 summarizes these tests.

Table 4: *SBI_{net}* Tests

Test	Purpose	Government/contractor role	Location
Developmental Testing	Verifies and validates the system's engineering process.	—	—
System Integration Testing	Consists of three types of tests (below).	Contractor performs	Laboratory
Component-level testing	Verifies the functional performance of individual components against component requirements.	Contractor performs	Laboratory
Interim-level integration testing	Verifies compatibility of individual interfaces of hardware and software components.	Contractor performs	Laboratory
System-level integration testing	Verifies that system requirements are met when subsystems are integrated with the COP software.	Contractor performs	Mostly laboratory, some field
System Verification Testing ^a	Verifies that the design being tested is compliant with the component or system requirements.	Contractor performs	Mostly laboratory, some field
System Acceptance Testing	Verifies that the installed system meets system requirements (i.e., the system functions as designed, performs as predicted in the deployed environment, and is ready for operational testing). Provides the basis for government accepting the system.	Contractor performs	Field
Operational Testing	Determines system operational effectiveness and suitability for the intended use by representative users in a realistic environment.	Government users and independent testers perform	Field

Source: GAO analysis of draft Test and Evaluation Master Plan.

^aCurrently referred to by the program office as "System Qualification Testing."

Limited Definition of SBInet Deployments, Capabilities, Schedule, and Life Cycle Management Process Increases Program's Exposure to Risk

Important aspects of SBInet 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 SBInet deployments and capabilities have continued to change since the program began and, even now, remain unclear. Further, the approach that is being used to define, develop, acquire, test, and deploy SBInet is similarly unclear and has continued to change. According to SBInet officials, schedule changes are due largely to an immature system design, and the lack of a stable development approach is due to insufficient staff and turnover. The absence of clarity and stability in these key aspects of SBInet introduces considerable program risks, hampers DHS's ability to measure program progress, and impairs the ability of the 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

One key aspect of successfully managing large IT programs, like SBInet, is establishing program commitments, including what capabilities are to be deployed and when and where they are to be deployed. Only when such commitments are clearly established can program progress be measured and can responsible parties be held accountable.

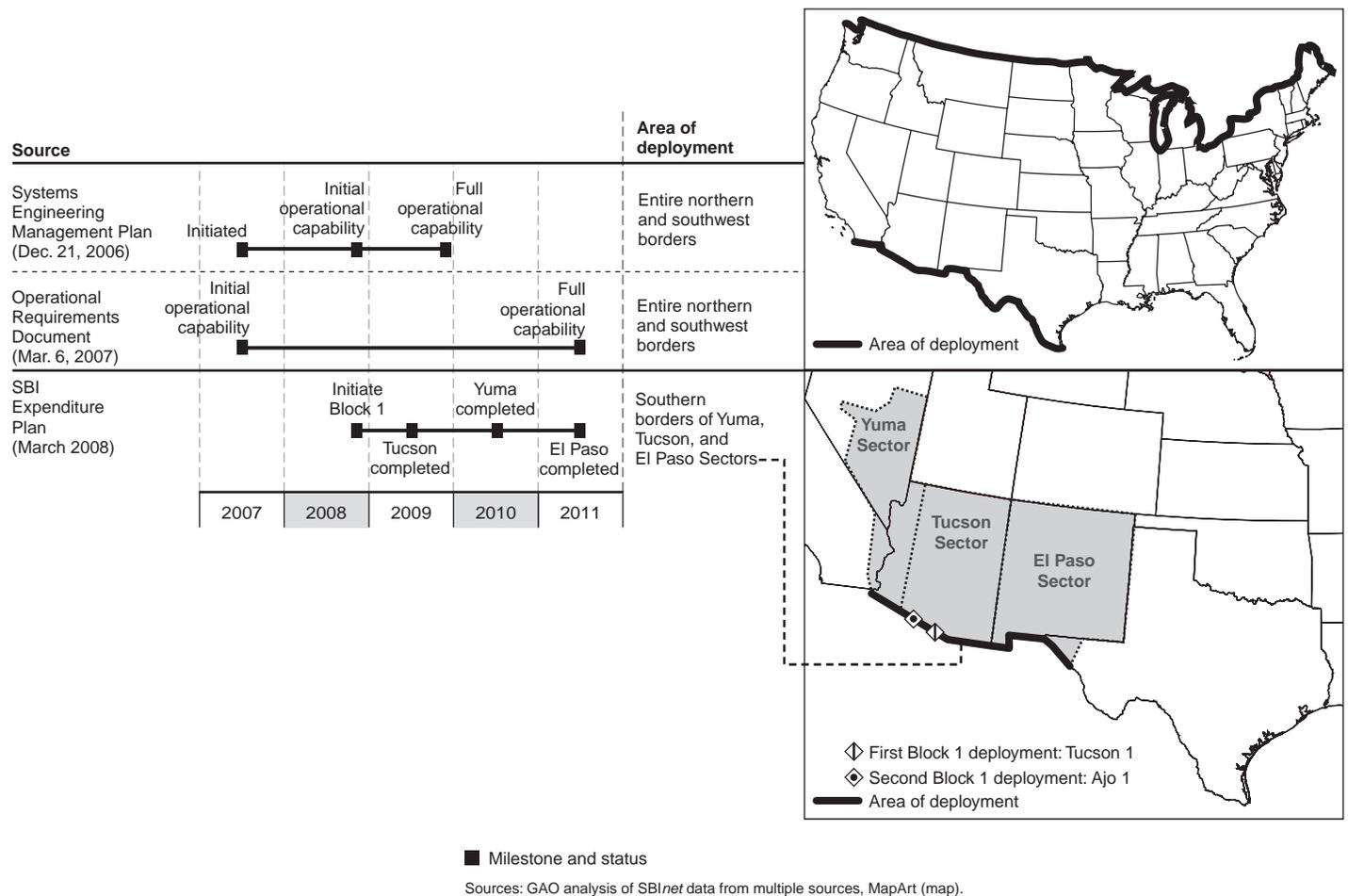
The scope and timing of planned SBInet deployments and capabilities that are to be delivered have not been clearly established, but rather have continued to change since the program began. Specifically, as of December 2006, the SBInet System Program Office planned to deploy an "initial" set of capabilities along the entire southwest border by late 2008 and planned to deploy a "full" set of operational capabilities along the southern and northern borders (a total of about 6,000 miles) by late 2009.¹² As of March 2007, the program office had modified its plans, deciding instead to deploy the initial set of capabilities along the southwest border by the end of fiscal year 2007 (almost a year earlier than originally planned) and delayed the deployment of the final set of capabilities for the southern and northern borders until 2011.

In March 2008, the program office again modified its deployment plans, this time significantly reducing the area to which SBInet capabilities are to

¹²DHS did not report these timeframes in its December 4, 2006, SBI Expenditure Plan. Rather, it reported that it planned to deploy SBInet to the southwest border by 2011 and did not provide a timeframe for deployment to the northern border.

be deployed. At this time, DHS planned to complete deployments to three out of nine sectors along the southwest border—specifically, to Tucson Sector by 2009, Yuma Sector by 2010, and El Paso Sector by 2011. According to program officials, other than the dates for the Tucson, Yuma, and El Paso Sectors, no other deployment dates have been established for the remainder of the southwest or northern borders. (Figure 5 shows the changes in the planned deployment areas.)

Figure 5: Changes in Planned Deployments over Time



The figure also shows the two sites within the Tucson Sector, Tucson 1 and Ajo 1, at which an initial Block 1 capability is to be deployed. Together, these two deployments cover 53 miles of the 1,989-mile-long southern border.¹³ According to the March 2008 SBI expenditure plan and agency documentation as of June 2008, these two sites were to have been operational by the end of 2008. However, as of late July 2008, program officials reported that the deployment schedule for these two sites has again been modified, and they will not be operational until “sometime” in 2009. According to program officials, the slippage in the deployment schedule is due to the need to complete environmental impact assessment documentation for these locations. 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.

Just as the scope and timing of planned deployments have not been clear and have changed over time, the specific capabilities that are to be deployed have been unclear. For example, in April 2008, program officials stated that they would not know which of the *SBI* requirements would be met by Block 1 until the Critical Design Review, which at that time was scheduled for June 2008. At that time, program officials stated that the capabilities to be delivered would be driven by the functionality of the COP. In June, the review was held, but according to available documentation, the government did not consider the design put forth by the contractor to be mature. As a result, the system design was not accepted in June as planned. Among the design limitations found was a lack of evidence that the system requirements were used as the basis for the Tucson 1 and Ajo 1 design, lack of linkage between the performance of surveillance components and the system requirements, and incomplete definition of system interfaces. As of late July 2008, these issues were unresolved, and thus the design still had not been accepted. In addition, in late July 2008, agency officials stated that the capabilities to be delivered will be driven by the functionality of the surveillance components, not the COP.

¹³The area that will be covered by Tucson 1 is similar to the area covered by Project 28 (sometimes referred to as “Block 0”); it is to include 23 of the 28 miles associated with Project 28. According to the System Program Office, the Project 28 capabilities (surveillance systems and COP) will be replaced with Block 1 capabilities as part of the Tucson 1 deployment.

In addition, the 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 have the mobile data terminals in border patrol vehicles, even though (1) such terminals are part of Project 28 capabilities and (2) workshops were held with the users in February 2008 and June 2008 to specifically define the requirements for these terminals for inclusion in Block 1. According to program officials, these terminals will not be part of Block 1 because the wireless communications infrastructure needed to support these terminals will not be available in time for the Tucson 1 deployment. Rather, they expect the wireless infrastructure to be ready “sometime” in 2009 and said that they will include the mobile data terminals in Block 1 deployments when the infrastructure is ready. Without the mobile data terminals, agents will not be able to obtain key information from their vehicles, such as maps of activity in a specific area, incident reports, and the location of other agents in the area. Instead, the agents will have to use radios to communicate with the sector headquarters to obtain this information.

In addition, program officials told us that a number of other requirements cannot be included in the Block 1 version of the COP, referred to as version 0.5, due to cost and schedule issues. However, we have yet to receive a list of these requirements. According to program officials, they hope to upgrade the COP in 2009 to include these requirements.

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

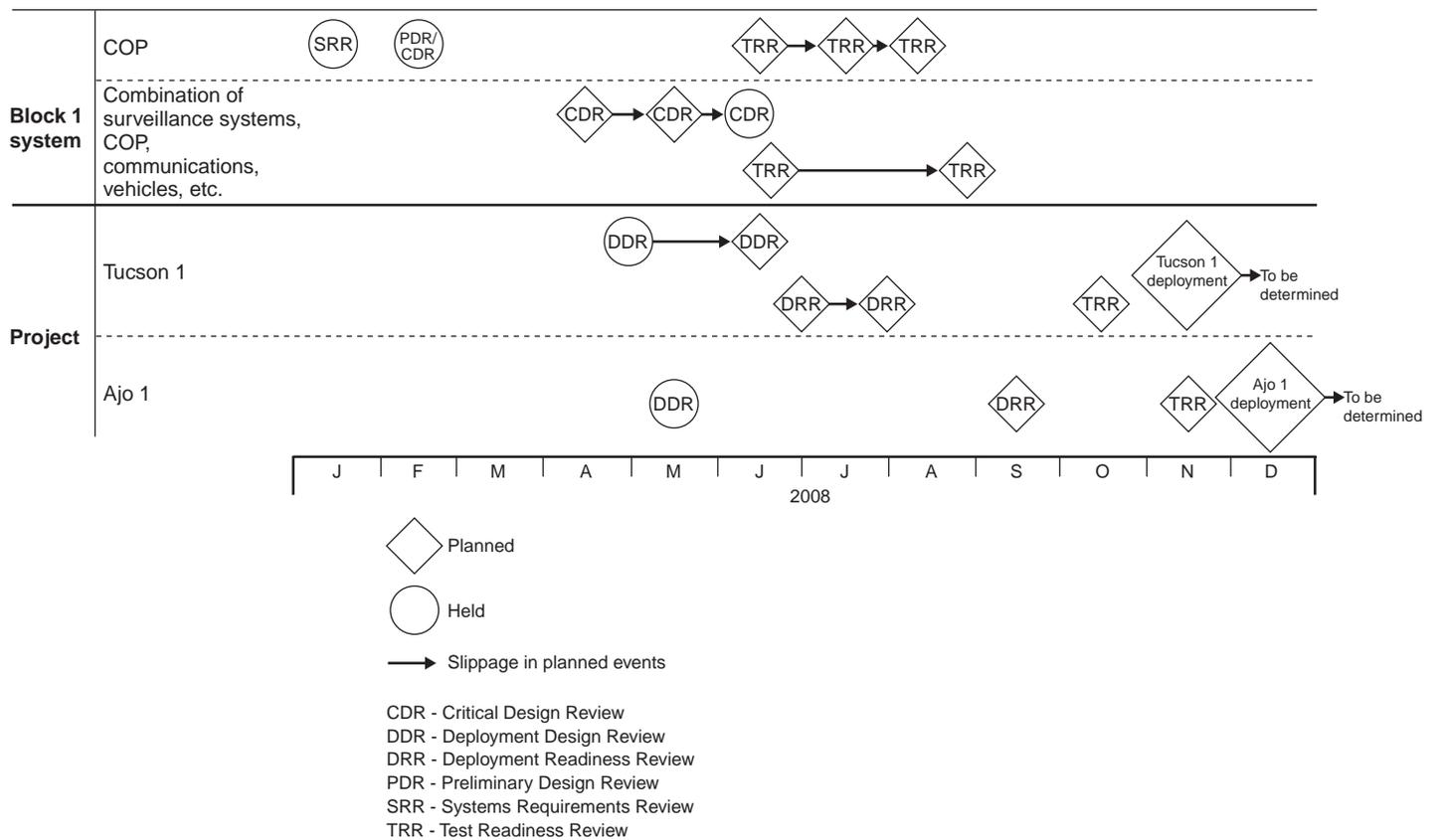
Another key aspect of successfully managing large programs like *SBI^{net}* is having a schedule that defines the sequence and timing of key activities and events and is realistic, achievable, and minimizes program risks. However, the program office does not yet have an approved integrated master schedule to guide the execution of *SBI^{net}*, and according to program officials, such a schedule has not been in place since late 2007. In the absence of an approved integrated master schedule, program officials stated in mid-August 2008 that they have managed the program largely using task-order-specific baselined schedules,¹⁴ and have been working to

¹⁴The program office is monitoring the individual schedules for five *SBI^{net}* task orders.

create a more integrated approach. A program official also stated that they have recently developed an integrated master schedule but that this schedule is already out of date and undergoing revision. For example, the deployment of the SBI^{net} system to the Tucson Sector will not be completed in 2009 as planned.

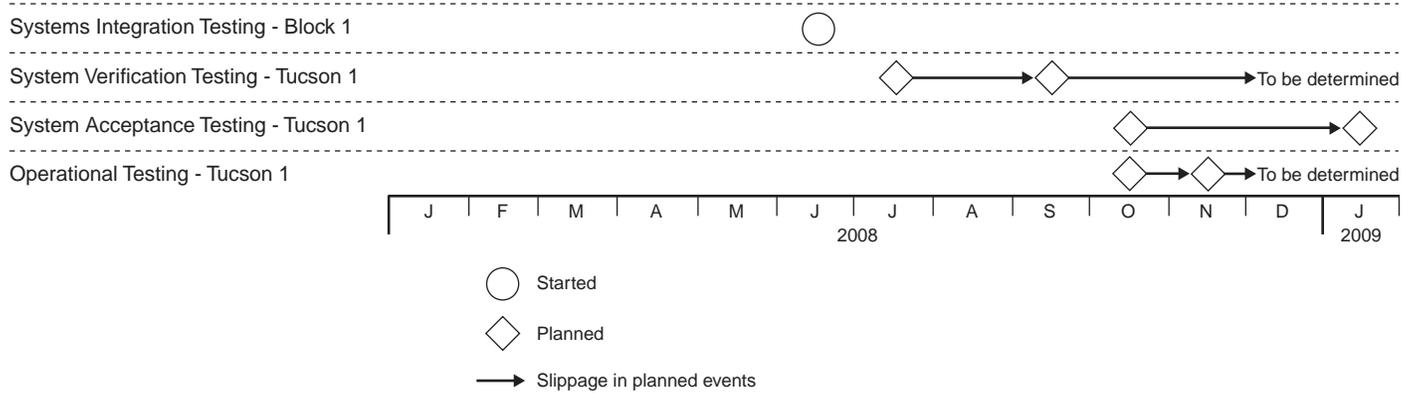
To understand where the program is relative to established commitments, we analyzed schedule-related information obtained from other available program documents, briefings, and interviews. In short, our analysis shows a schedule in which key activities and events are subject to constant change, as depicted in the following two figures. Figure 6 shows the changes to the schedule of planned and held reviews and anticipated deployment dates, and figure 7 shows the changes to the schedule of testing activities.

Figure 6: Changes in Schedules for Reviews and Deployment



Source: GAO analysis of SBI^{net} data from multiple sources.

Figure 7: Changes in Schedules for Testing



Source: GAO analysis of SBInet data from multiple sources.

In May 2008, program officials stated that the schedule changes were due largely to the fact that the contractor had not yet provided a satisfactory system-level design. They also noted that the contractor’s workforce has experienced considerable turnover, including three different program managers and three different lead system engineers. They also stated that the System Program Office has experienced attrition, including turnover in the SBInet 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.

SBInet 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 processes followed in developing and acquiring the system. To the extent that a system’s life cycle management approach and related development and acquisition processes are well-defined, the chances of delivering promised system capabilities and benefits on time and within budget are increased. To be well-defined, the approach and processes should be fully documented, so that they can be understood and properly implemented by those responsible for doing so.

The life cycle management approach and processes being used by the SBInet 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. Moreover, in discussions with agency officials to clarify our understanding of these processes, new terms and processes have been routinely introduced, indicating that the processes are continuing to evolve. Agency officials acknowledge that they are still learning about and improving their processes. Without a clearly documented and universally understood life cycle management approach and supporting processes, the program is at increased risk of not meeting expectations.

Key program documentation that is to be used to guide acquisition and development activities, including testing and deployment activities, is incomplete, even though *SBI*net acquisition and development are already under way. 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 are lacking sufficient information to clearly guide system activities, as the following examples explain:

- The Systems Engineering Plan includes a diagram of the engineering process; however, the steps of the process and the gate reviews are not defined or described in the text of the document. For example, this document does not contain sufficient information to understand what occurs at key reviews, such as the Preliminary Design Review, the Critical Design Review, and the Test Readiness Review.
- The Test and Evaluation Master Plan describes in more detail some of the reviews that are not described in the Systems Engineering Plan, but the reviews included are not consistent between the documents. For example, the Test and Evaluation Master Plan includes a System Development and Demonstration Review that is not listed in the Systems Engineering Plan. In addition, it is not clear from the Test and Evaluation Master Plan how the reviews fit into the overall engineering process.

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. Moreover, these descriptions were not always consistent with what was contained in the documentation, as the following examples demonstrate:

-
- Component testing is not described in the Test and Evaluation Master Plan in a manner consistent with how officials described this testing. Specifically, while the plan states that components will be tested against the corresponding component requirements to ensure all component performance can be verified, program officials stated that not all components will undergo component testing. Instead, they said that testing is not required if component vendors submit a certificate of compliance for certain specifications.
 - Functional qualification testing was described to us by program officials in July 2008 as a type of testing to be performed during software development activities. However, this type of testing is not defined in available program documentation, and it was not included in any versions of the documentation associated with the life cycle management approach and related engineering processes.
 - Certain reviews specified in documentation of the life cycle management process are not sufficiently defined. For example, the Systems Engineering Plan shows a Production Readiness Review as part of the system-level process and an Operational Readiness Review as part of the project-level process. However, program officials stated that these reviews are not completely relevant to *SBI_{net}* because they are targeted for informational systems rather than tactical support systems, such as *SBI_{net}*. According to the officials, they are in the process of determining how to apply the reviews to *SBI_{net}*. For example, in July 2008, officials reported that they may move the Production Readiness Review from the system-level set of activities, as shown in the Systems Engineering Plan, to the project-level set of activities. Program officials also stated that they are working to better define these reviews in the Systems Engineering Plan.

Program officials told us that the *SBI_{net}* life cycle management approach and related engineering processes are understood by both government and contractor staff 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 project with different acquisition backgrounds, and that they are still learning about, evolving, and improving the approach and processes. According to these officials, a revised and updated Systems Engineering Plan should be finalized by September 2008.

The lack of definition and stability in the approach and related processes being used to define, design, develop, acquire, test, and deploy *SBI_{net}* introduce considerable risk that both the program officials and contractor staff will not understand what needs to be done when, and thus that the program will not consistently employ disciplined and rigorous methods. Without the use of such methods, the risk of delivering a system that does not meet operational needs and does not perform as intended is increased. Moreover, without a well-defined approach and processes, it is difficult to gauge progress and thus promote performance and accountability for results.

Limitations of *SBI_{net}* Requirements Development and Management Efforts Increase Program Risk

Well-defined and managed requirements are a cornerstone of effective system development and acquisition. According to recognized guidance,¹⁵ documenting and implementing a disciplined process for developing and managing requirements can help reduce the risks of developing a system that does not meet user needs, cannot be adequately tested, and does not perform or function as intended. Such a process includes, among other things, eliciting user needs and involving users in the development process; ensuring that requirements are complete, feasible, verifiable, and approved by all stakeholders; documenting and approving the requirements to establish a baseline for subsequent development and change control; and ensuring that requirements are traceable both back to operational requirements and forward to detailed system requirements and test cases.

To the program office's credit, it recently developed guidance for developing and managing requirements that is consistent with recognized leading practices. For example, the program's guidance states that a requirements baseline should be established and that requirements are to be traceable both back to higher-level requirements and forward to verification methods. However, this guidance was not finalized until February 2008 and thus was not used in performing a number of key requirements-related activities.

¹⁵The Capability Maturity Model® Integration for Development, developed by the Software Engineering 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. Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Development, Version 1.2 (Pittsburgh, Penn., August 2006).

In the absence of well-defined guidance, the program's efforts to implement leading practices for developing and managing requirements have been mixed. For example, while the program has elicited user needs as part of its efforts to develop high-level operational requirements, it has not baselined all requirements. Further, it has not ensured that the operational requirements were, for example, verifiable, and it has not made certain that all of the different levels of requirements are aligned to one another. 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.

Requirements Development and Management Guidance Is Consistent with Leading Practices but Was Developed After Many Requirements Activities Were Performed

The *SBI*net program office has developed guidance for developing and managing requirements that is generally consistent with recognized leading practices. According to these practices, effectively developing and managing requirements includes, among other things, eliciting users' needs early in the development process and involving them throughout the process; ensuring that requirements are complete, feasible, verifiable, and approved by all stakeholders; documenting and approving the requirements to establish a baseline for subsequent development and change control; and ensuring that requirements are traceable both back to operational requirements and forward to detailed system requirements and test cases.

In February 2008, the program office approved its *SBI*net Requirements Development and Management Plan. According to the plan, its purpose is to describe a comprehensive approach to developing and managing requirements for the *SBI*net program. Our analysis of this plan shows that it is consistent with leading practices. For example, the plan states that

- users should provide input to the requirements definition process through early and ongoing participation in integrated product teams, user conferences, and other requirements-gathering and verifying activities;
- requirements developers are to ensure that requirements are complete, unambiguous, achievable, verifiable, and not redundant;
- a requirements baseline should be created to provide a common understanding of the system to be built and to prevent deviations to the requirements from entering during design, development, or testing; and
- bidirectional traceability both back to higher-level requirements and forward to detailed test methods should be established and maintained

and that the requirements management team is responsible for maintaining the requirements management database and holding the contractor responsible for any traceability issues.

Moreover, the plan defines procedures and steps for accomplishing each of these goals. For example, the procedure for requirements development outlines the purpose of the procedure, who is involved, what documentation is necessary to begin the procedure, and what outputs are expected at the end. The procedure then describes 16 steps necessary to achieve the requirements development activities. A separate procedure is provided for requirements verification and validation.

However, the plan was not approved until after key *SBI*net requirements documents were written and baselined. Specifically, user operational requirements were approved and baselined in March 2007; system requirements were first baselined in March 2007; and several component requirements were baselined in June, August, and October 2007. As a result, the plan was not used to guide these requirements development and management efforts.

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

As noted above, one of the leading practices associated with effective requirements development and management is engaging system users early and continuously. In doing so, the chances of defining, designing, and delivering a system that meets their needs and performs as intended are increased.

In developing the operational requirements, the System Program Office involved *SBI*net users in a manner that is consistent with leading practices and that reflects lessons learned from Project 28. Specifically, it conducted requirements-gathering workshops from October 2006 through April 2007 to ascertain the needs of Border Patrol agents. In addition, it established work groups in September 2007 to inform the next revision of the operational requirements by soliciting input from both the Office of Air and Marine Operations and the Office of Field Operations. Further, to develop the COP technology for *SBI*net, the program office is following a software development methodology that allows end users to be directly

involved in software development activities and, thereby, permits software solutions to be tailored to users' needs.¹⁶

Through such efforts to identify and elicit user needs in developing high-level requirements, the chances of developing a system that will meet user needs are increased.

Not All Levels of Requirements Have Been Adequately Baseline

The creation of a requirements baseline is important for providing a stable basis for system design, development, and testing. Such a 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. Until requirements are baselined, they remain unclear and subject to considerable and uncontrolled change, which in turn makes system design, development, testing, and deployment efforts equally uncertain. 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, since the requirements are intended to inform, guide, and constrain the system's design.

For *SBI*net, while many of the requirements have been baselined, two types have not yet been baselined. According to the System Program Office, the operational requirements and the system requirements were approved and baselined in March 2007. In addition, various system component requirements were baselined in June, August, and October of 2007. However, the program had not baselined its COP software requirements as of July 2008, although according to program officials, the COP has been designed and is under development. Further, it has yet to baseline its project-level requirements, which define the requirements for the system configuration to be deployed to a specific geographical area, such as Tucson 1.

With respect to the COP, requirements for the software and hardware had not been baselined as of the end of July 2008, despite the fact that a combined Preliminary Design Review and Critical Design Review for the COP was held in February 2008 and a Critical Design Review for the

¹⁶This method, Rapid Application Development and Joint Application Design (RAD/JAD), uses graphical user interfaces and direct-end-user involvement in a collaborative development approach.

system as whole was held in June 2008. According to agency officials and the *SBI*net Requirements Development and Management Plan, requirements should be baselined before the Critical Design Review. Regardless, program officials state that the contractor has developed several “builds” (i.e., versions) of the COP, which are currently being tested. According to program officials, the requirements were not complete because certain interface requirements¹⁷ had not yet been completely identified and defined. Without baselined requirements, the basis of the system design and the degree to which it satisfies requirements are unclear. Moreover, the risk of the design not aligning to requirements is increased. According to the results of the Critical Design Review, this risk was realized. Specifically, the System Program Office notified the contractor that there was no evidence linking the performance of surveillance components to the system requirements, that the review could not be completed until the interface requirements had been finalized, and that a mature design had not been presented at the review.

With respect to project-level (i.e., geographic area) deployment requirements, baselined requirements do not yet exist. Specifically, requirements for the Tucson Sector, which includes Tucson 1 and Ajo 1, have yet to be baselined. According to the *SBI*net Requirements Development and Management Plan, requirements should be baselined before the Project Requirements Review, and a new requirements baseline should be created following the subsequent Deployment Design Review. However, project-level requirements were not baselined at a Project Requirements Review held for the Tucson Sector Project in March 2007 or at a Deployment Design Review in June 2007. Officials stated that this is because the plan was not approved until February 2008 and thus was not in effect. However, since the plan became effective, Deployment Design Reviews were held for Tucson 1 and Ajo 1 in April 2008 and May 2008, respectively, but the project-level requirements were not baselined.

Despite the absence of baselined requirements, the System Program Office has proceeded with development, integration, and testing activities for the Block 1 capabilities to be delivered to Tucson 1 and Ajo 1. As a result, it faces an increased risk of deploying systems that do not align well with requirements and thus may require subsequent rework. The lack of project requirements has already had an effect on testing activities. Specifically,

¹⁷Interface requirements describe the capabilities that must be in place in order to integrate components and products together.

the draft system integration test plan notes that, without project requirements, testing will have to be guided by a combination of other documents, including engineering development requirements, related component requirements, and architectural design documents.

Baselined Operational Requirements Used to Inform Lower-Level Requirements Are Limited

As stated above, one of the leading practices for developing and managing requirements—which is reflected in the program office’s own plan—is that requirements should be sufficiently analyzed to ensure that the requirements are, among other things, complete, unambiguous, and verifiable. However, an independent review of *SBI*net operational requirements reported numerous problems. Specifically, a review of the *SBI*net program commissioned by the Office of the Deputy Secretary of Homeland Security found that several requirements were unaffordable and unverifiable. Examples of these requirements include the following:

- Allow for complete coverage of the specified area or zone to be surveilled.
- Maximize intended deterrence and minimize countermeasure effectiveness.
- Function with high reliability under reasonably foreseeable circumstances.
- Reliably provide the appropriate power and bandwidth at the least cost that will support the demand.

In April 2008, a program official stated that the operational requirements document is currently being rewritten to address concerns raised by this review. For example, we were told that certain system performance requirements are being revised in response to a finding that the requirements are insufficient to ensure delivery of a properly functioning system. Program officials stated that they expect to finalize the revised operational requirements document in October 2008.

However, given the number and types of problems associated with the operational requirements—which are the program’s most basic customer requirements and form the basis for all lower-level requirements—it is unclear how the system, component, and software requirements can be viewed as verifiable, testable, or affordable. Until these problems are addressed, the risk of building and deploying a system that does not meet mission needs and customer expectations is increased, which in turn increases the chances of expensive and time-consuming system rework.

SBI*net* Requirements Have Not Been Sufficiently Aligned

As noted above, one of the leading practices 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, stating that a traceability relationship should exist among the various levels of requirements. For example, it states that operational requirements should trace to the system requirements, which in turn should trace to component requirements. Further, it states that component requirements should trace to design requirements and to a verification method. In addition, the SBI*net* System Program Office established detailed guidance¹⁸ for populating and maintaining the requirements database for maintaining linkages among the various levels of requirements and test verification methods.

To provide for requirements traceability, the prime contractor established such a requirements management database. However, the reliability of the requirements in this database is questionable, and the SBI*net* System Program Office has not effectively overseen the contractor's management of requirements through this database. Specifically, 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. See table 5 for the failure rates for each of our tracing analyses, along with the related confidence intervals.

¹⁸SBI*net* Requirements Management Plan, January 15, 2007.

Table 5: SBInet Requirements Traceability Results

Traceability links from component requirement	Estimated failure rate	95 percent confidence interval
To system requirement and then to operational requirement	76%	64–86%
To system requirement	48	34–61
To verification method	20	11–33
To design requirement	100	95–100

Source: GAO analysis of program office data.

While program officials could not explain the reason for this lack of traceability in most cases, they did attribute the 100-percent failure in tracing component requirements to the design requirements to the absence of any design requirements in the program office’s copy of the database.

A contributing factor to the program office’s inability to explain why requirements were not traceable is its limited oversight of the contractor’s efforts to manage requirements through this database. According to program officials, the contractor created the SBInet requirements management database in December 2006, but the program office did not receive a copy of the database until March 2008, despite requests for it beginning in fall 2007. In early May 2008, the Chief Engineer told us the contractor had been reluctant to provide the database because it viewed the database’s maturity level as low. Moreover, the program office’s direct access to the database had not been established because of security issues, according to this official.

Following our efforts to trace requirements, the program office obtained direct access to the contractor’s database and initiated efforts with the contractor to resolve the traceability gaps. However, program officials told us that they are still not certain that the database currently contains all of the system requirements or even the reduced Block 1 system requirements. As a result, they did not rely on it during the recent Critical Design Review to verify requirements traceability. Instead, they said that manual tracking methods were used.

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.

As a result, the risk of expensive and time-consuming system rework is increased.

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, among other things, having an overarching test plan or strategy as a basis for managing system testing, developing well-defined and approved plans for executing testing activities, and testing individual system components to ensure that they satisfy defined requirements prior to integrating them into the overall system.

The SBI^{net} System Program Office is not effectively managing its testing activities. Specifically, it has not tested individual system components prior to integrating these components with other components and the COP software. In addition, although the program's draft Test and Evaluation Master Plan is currently being used as the program's overall strategy to manage SBI^{net} testing, the plan is incomplete and unclear with respect to several test management functions. As a result, the chances of SBI^{net} testing being effectively performed are reduced, which in turn increases the risk that the delivered and deployed system will not meet operational needs and not perform as intended.

System Integration Testing Has Not Been Adequately Planned or Executed

To be effectively managed, relevant federal guidance¹⁹ states that testing should, among other things, be governed by a well-defined and approved plan, and it should be executed in accordance with this plan. Further, integration testing should be preceded by tests of system components (whether acquired or developed) that are to be integrated to form the overall system. Once the components are tested to ensure that they satisfy defined requirements, the integrated system can be tested to verify that it performs as required. For SBI^{net}, this has not occurred. As a result, the risk of the system not meeting operational needs and not performing as intended is increased, which in turn is likely to introduce the need for expensive and time-consuming system rework.

The SBI^{net} Systems Program Office reports that it began Block 1 system integration testing in June 2008. However, it still does not have an approved system integration test plan. Specifically, the system's Critical

¹⁹See, for example, [GAO/AIMD-10.1.21](#).

Design Review, which was held in June 2008, found numerous problems with the contractor's plan for system integration testing, and as a result, the program office did not accept the plan. Examples of problems were that the test plan refers to other test plans that the contractor had yet to deliver and the plan identified system components that were not expected to be part of Block 1. As a result, the program office decided that the system integration plan needed to be revised to document and describe the full set of actual testing activities that were to occur, including identifying where and to what level the different phases of integration tests would occur.

Notwithstanding these problems and the absence of an approved plan, the contractor began integration testing in June 2008. According to program officials, this was necessary to meet the tight time frames in the schedule. However, without an accepted system integration test plan in place, testing cannot be effectively managed. For example, the adequacy of the test scope cannot be assured, and the progress in completing test activities cannot be measured. As a result, there is an increased risk that the delivered system will not meet operational needs and will not perform as intended and that expensive and time-consuming system rework will be required.

Moreover, the *SBI*net draft Test and Evaluation Master Plan describes system integration testing as first testing individual components to verify that the smallest defined module of a system works as intended (i.e., meets functional and performance requirements). This allows defects with individual components to be identified and corrected before they are integrated with other system components. Once the components are tested, their respective hardware and software interfaces are to be tested before subsystems are tested in combination with the COP software. Such an incremental approach to testing permits system defects to be found and addressed before system components are integrated and component problems become more expensive and time-consuming to correct.

However, 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 stated that the contractors' self-certification that the components meet functional and performance requirements was acceptable. However, this approach is not

consistent with the Test and Evaluation Master Plan. Moreover, program officials acknowledged that this approach did not verify if the individual components in fact met requirements. Nevertheless, they said that they have recently modified their definition of component testing to allow the contractor's certification to be used.

In our view, relying solely on contractor certification is not a sufficient substitute for component testing—as defined in the Test and Evaluation Master Plan—because it increases the risk that components, and thus the entire system, will not perform as intended. This risk is already starting to be realized. Specifically, the results of the Block 1 Critical Design Review performed in early in June 2008 show that design documents did not link components' performance to the system requirements.

Key Test Management Activities Have Not Been Adequately Defined and Addressed

To ensure that system testing is effectively performed, federal guidance provides for having an overarching test plan or strategy to use as a basis for managing system testing. Among other things, 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 and to ensure that test progress can be tracked and results can be reported and addressed. The plan should also define the roles and responsibilities of the various groups responsible for different levels of testing and include a description of how the test organization manages and oversees these groups in their activities.

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. As of July 2008, program officials told us that they did not expect the draft plan to be approved until August 2008, even though testing activities began in June 2008.²⁰

Moreover, the draft Test and Evaluation Master Plan is not complete. For example, it does not contain an accurate and up-to-date test schedule with milestones and completion dates for all levels of test activities. Rather, the schedule information included in the plan has been overtaken by events, to the point that program officials stated that many of the dates on the

²⁰DHS stated in agency comments that it plans to revise and approve the Test and Evaluation Master Plan by December 31, 2008.

schedules have changed or are not accurate. Moreover, they described attempting to have an accurate schedule of testing activities and events as “futile” because the program’s schedule is constantly changing. As another example, the draft Test and Evaluation Master Plan does not identify any metrics for measuring testing progress for any type of testing to be performed. According to federal guidance, an accurate schedule is necessary to inform planning for and sequencing of each type of testing to be performed, including ensuring that test resources are available when needed and that predecessor test events occur before successor events begin. This guidance also states that without performance metrics, it is difficult to understand where test activities stand and what they show in a manner that can inform program decision making.

As another example, the draft Test and Evaluation Master Plan does not clearly define the roles and responsibilities of various entities that are involved in system testing. Specifically, the plan identifies seven entities, but it only provides vague descriptions of their respective roles and responsibilities that are not meaningful enough to effectively guide their efforts. For example, the plan identifies two entities that are to be involved in operational testing: the DHS Science and Technology Test and Evaluation Office and the U.S. Army Test and Evaluation Command. According to the plan, the DHS office is to function as the operational test authority and will be responsible for initial planning of “dedicated initial” and “follow-on” operational testing and evaluation, and the Army group is to conduct operational testing. With no further clarification, it is not clear what is expected of each of these entities, including how they are to interact. Table 6 lists each of the identified entities and provides their respective roles and responsibilities copied from the draft plan.

Table 6: Roles and Responsibilities of Entities Identified in the Draft SBInet Test and Evaluation Master Plan

Entity	Roles and responsibilities as defined in plan
System Prime Contractor	<ul style="list-style-type: none"> • Conducts developmental testing (e.g., component acceptance testing, system integration testing, and verification and validation of performance).
U.S. Army Test and Evaluation Command	<ul style="list-style-type: none"> • Conducts sample System Prime verification testing. • Conducts operational testing. • Gathers field data to assess the degree to which SBInet achieves mission needs.
U.S. Customs and Border Protection	<ul style="list-style-type: none"> • Provides operational feedback using defined metrics that are to be used to identify and evaluate necessary SBInet Concept of Operations modifications.
Independent Verification and Validation agent	<ul style="list-style-type: none"> • Provides CBP with objective third party evaluation of the C3I development to verify system design and applications meet C3I requirements.
DHS Science and Technology Test and Evaluation Office	<ul style="list-style-type: none"> • Functions as the Operational Test Authority, including initial planning of dedicated Initial Operational Test and Evaluation and Follow-on Operational Test and Evaluation.
Program Test and Evaluation Integrated Project Teams	<ul style="list-style-type: none"> • Provides technical expertise to the System Prime Integrated Project Teams. • Provides expertise in test plan review and test observation.
SBInet System Program Office Test and Evaluation Division	<ul style="list-style-type: none"> • Develops test and evaluation reports.

Source: SBInet data.

Besides being vague, the descriptions of roles and responsibilities are also incomplete and not consistent with other program documents. For example, according to the draft plan, the Test and Evaluation Division of the SBInet System Program Office is responsible only for developing test and evaluation reports. However, according to the draft SBInet Systems Engineering Plan, this entity is to act as a subject matter expert for the oversight or conduct of various testing activities.

Beyond this lack of clearly defined roles and responsibilities, there are other problems with the groups assigned testing roles. First, some of the entities identified in the draft plan are not yet operational and thus are unavailable to participate and perform their assigned roles and responsibilities. According to program officials, the independent verification and validation agent has not been selected, the Integrated Project Teams have not been chartered, and DHS is still in the process of establishing the DHS Science and Technology Test and Evaluation Office. Second, although CBP has an interagency agreement with the U.S. Army Test and Evaluation Command for operational testing, no such agreement exists with the SBInet program specifically for Block 1 testing.

Finally, neither the draft Test and Evaluation Master Plan nor the draft Systems Engineering Plan clearly defines the program office’s role and responsibilities for managing and overseeing each of the other six test entities and their respective test activities. The SBInet System Program

Office is responsible and accountable for ensuring that the system is successfully deployed and operates as intended. Given the criticality of testing in ensuring a successful program, this means that the program office must ensure that each of these entities executes its assigned roles effectively. However, the draft Test and Evaluation Master Plan does not recognize this role and its associated responsibilities. Further, while the draft Systems Engineering Plan states that the program office is responsible for engaging external test agents, it provides no further description of the program office's roles and responsibilities.

Without clearly defined roles and responsibilities for all entities involved in *SBI*net testing, the risk of test activities not being effectively and efficiently performed increases. As a result, the chances are increased that the deployed system will not meet operational requirements and perform as intended. Ultimately, this could lead to expensive and time-consuming system rework.

Conclusions

A fundamental aspect of successfully implementing a large 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 by adequately defining the approach and processes to be used in delivering these commitments, 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 key 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 are significant in that they increase the risk that the delivered system solution will not meet user needs and operational requirements and will not perform as intended. These consequences, in turn, increase the chances that the system will require expensive and time-consuming rework. In light of these circumstances and

risks surrounding *SBI_{net}*, it is important for the program office to reassess its approach to and plans for the program—including its associated exposure to cost, schedule, and performance risks—and to disclose these risks and alternative courses of action for addressing them to DHS and congressional decision makers. It is also important for the program to correct the weaknesses discussed in this report surrounding the program’s unclear and constantly changing commitments and its life cycle management approach and processes, including the processes and efforts performed to date relating to requirements development and management and testing.

While doing so will not guarantee a successful program, it will minimize the program’s exposure to risk and thus decrease 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.

Recommendations for Executive Action

To improve DHS’s efforts to acquire and implement *SBI_{net}* we are making eight recommendations.

To permit meaningful measurement and oversight of and accountability for the program, we recommend that the Secretary of Homeland Security direct the CBP Commissioner to ensure that (1) the risks associated with planned *SBI_{net}* acquisition, development, testing, and deployment activities are immediately assessed and (2) the results, including proposed alternative courses of action for mitigating the risks, are provided to the Commissioner and DHS’s senior leadership, as well as to the department’s congressional authorization and appropriation committees.

We further recommend that the Secretary of Homeland Security direct the CBP Commissioner to have the Acting *SBI_{net}* Program Manager take the following additional actions:

- 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.
- Finalize and approve an integrated master schedule that reflects the timing and sequencing of the work needed to achieve these commitments.

-
- Revise and approve versions of the *SBI*net life cycle management approach, including the draft Systems Engineering Plan and draft Test and Evaluation Management Plan, and in doing so, ensure that these revised and approved versions are consistent with one another, reflect program officials' recently described changes to the engineering and testing approaches, and reflect relevant federal guidance and associated leading practices.
 - Ensure that the revised and approved life cycle management approach is fully implemented.
 - Implement key requirements development and management practices to include (1) baselining requirements before system design and development efforts begin; (2) analyzing requirements prior to being baselined to ensure that they are complete, achievable, and verifiable; and (3) tracing requirements to higher-level requirements, lower-level requirements, and test cases.
 - Implement key test management practices to include (1) developing and documenting test plans prior to the start of testing; (2) conducting appropriate component level testing prior to integrating system components; and (3) approving a test management strategy that, at a minimum, includes a relevant testing schedule, establishes accountability for testing activities by clearly defining testing roles and responsibilities, and includes sufficient detail to allow for testing and oversight activities to be clearly understood and communicated to test stakeholders.

Agency Comments and Our Evaluation

In written comments on a draft of this report, signed by the Director, Departmental GAO/Office of Inspector General Liaison and reprinted in appendix II, the department stated that it agrees with seven of our eight recommendations, and partially disagrees with one aspect of the remaining recommendation. The department also stated that our report is factually sound and that it is working to address our recommendations and resolve the management and operational challenges identified in the report as expeditiously as possible. In this regard, it described actions recently completed, underway, and planned that it said addresses our recommendations. It also provided technical comments that we have incorporated in the report, as appropriate.

Regarding our recommendation to implement key test management practices, including conducting appropriate component-level testing prior to integrating system components, DHS commented that its current test strategy provides for the appropriate degree of technical confidence for

commercially available products, as evidenced by either certificates of conformance from the original equipment manufacturer, test documentation from independent government laboratories, or the prime contractor's component/integration level testing. We support DHS's current test strategy, as it is consistent with our recommendation. Specifically, it expands on the department's prior strategy for component testing, which was limited to manufacturer self-certification of component conformance and informal observations of system components, by adding the use of independent government laboratories to test the components. We would emphasize, however, that regardless of the method used, it is important that confidence be gained in components prior to integrating them, which our recommendation recognizes. As our report states, component-level testing was not performed for Block 1 components prior to initiating integration testing. Federal guidance and the *SBI_{net}* program office's own Test and Evaluation Master Plan recognize the need to first test individual components to verify that the system modules work as intended (i.e., meet functional and performance requirements) before conducting integration testing. By adopting such a hierarchical approach to testing, the source of any system defects can be discovered and isolated sooner rather than later, thus helping to avoid the potential for expensive and time-consuming system rework.

We are sending copies of this report to the Chairmen and Ranking Members of the Senate and House Appropriations Committees and other Senate and House committees and subcommittees that have authorization and oversight responsibilities for homeland security. We will also send copies to the Secretary of Homeland Security, the Commissioner of U.S. Customs and Border Protection, and the Director of the Office of Management and Budget. In addition, this report will be available at no cost on the GAO Web site at <http://www.gao.gov>.

Should your offices have any questions on matters discussed in this report, please contact me at (202) 512-3439 or at hiter@gao.gov. Contact points for our Office of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix III.

A handwritten signature in black ink, reading "Randolph C. Hite". The signature is written in a cursive style with a large initial "R" and a stylized "H".

Randolph C. Hite
Director, Information Technology Architecture
and Systems Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine whether the Department of Homeland Security (DHS) (1) has defined the scope and timing of planned *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 determine the extent to which DHS has defined the scope and timing of planned *SBI_{net}* capabilities and how these capabilities will be developed and deployed, we reviewed program documentation, such as the draft Systems Engineering Plan, the Systems Engineering Management Plan, the Operational Requirements Document, the Mission Engineering Process, the draft Test and Evaluation Master Plan, and the 2008 SBI Expenditure Plan to understand the *SBI_{net}* engineering process and the scope and timing of planned deployments. We also interviewed *SBI_{net}* officials and contractors to gain clarity beyond what was included in the program documentation and to obtain schedule information in the absence of an integrated master schedule for the program.

To determine if DHS is effectively defining and managing *SBI_{net}* requirements, we reviewed relevant documentation, such as the Requirements Development and Management Plan, the Requirements Management Plan, the Configuration and Data Management Plan, the Operational Requirements Document, System of Systems A-Level Specification, B-2 Specifications, and Vendor Item Control Drawings, and compared them to industry best practices¹ to determine the extent to which the program has effectively managed the systems requirements and maintained traceability backwards to high-level operational requirements and system requirements, and forward to system design and verification methods.

To assess reliability of the requirements data, we reviewed quality and access controls of the requirements database. We then randomly selected 59 requirements from a sample of 1,666 component requirements and traced them backwards to the system requirements and then to the operational requirements and forward to design requirements and verification methods. Because we followed a probability procedure based on random selection, we are 95 percent confident that each of the confidence intervals in this report will include the true values in the study

¹Carnegie Mellon Software Engineering Institute, Capability Maturity Model[®] Integration for Development, Version 1.2 (Pittsburgh, Penn., August 2006).

population. We used statistical methods appropriate for audit compliance testing to estimate 95 percent confidence intervals for the traceability of requirements in our sample. In addition, we interviewed program and contractor officials involved in requirements management to understand their roles and responsibilities. We also visited a contractor development facility in Huntsville, Alabama, to understand the contractor's role in requirements management and development and the use of its requirements management tool, known as the Dynamic Object-Oriented Requirements System (DOORS). In addition, we attended a demonstration of *SBI*net Rapid Application Development/Joint Application Design to understand how the users are involved in developing requirements.

To determine if DHS is effectively managing *SBI*net testing, we reviewed relevant documentation, such as the *SBI*net Test and Evaluation Master Plan, the Systems Integration Test Plan, the Quality Assurance Surveillance Plan, the Requirements Verification Plan, the Characterization Test Plan, and the Prime Mission Product Design, and compared them to relevant federal guidance² to determine the extent to which the program has effectively managed its testing activities. We also interviewed *SBI*net officials to gain clarity beyond what was included in the program documentation and to obtain schedule information in the absence of a formal testing schedule. In addition, we visited a contractor facility in Huntsville, Alabama, to better understand the contractor's role in testing activities and to observe the test lab and how testing is performed.

In addition, we visited the Tucson Sector Border Patrol Headquarters in Tucson, Arizona, to see the technology that was deployed as a prototype to understand the scope of the technology, how the Border Patrol agents use the technology, and future plans.

To assess data reliability, we reviewed related program documentation to substantiate data provided in interviews with knowledgeable agency officials, where available. For the information contained in the DHS independent study on *SBI*net, we interviewed the individuals responsible for conducting the review to understand their methodology, and determined that the information derived from this study was sufficiently

²GAO, *Year 2000 Computing Crisis: A Testing Guide*, [GAO/AIMD-10.1.21](#) (November 1998).

reliable for the purposes of this report. We have made appropriate attribution indicating the data's sources.

We performed our work at the U.S. Customs and Border Protection headquarters and contractor facilities in the Washington, D.C., metropolitan area; the Tucson Sector Border Patrol headquarters in Tucson, Arizona; and a contractor facility in Huntsville, Alabama. We conducted this performance audit from August 2007 to September 2008 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.

Appendix II: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

September 9, 2008

Mr. Randolph C. Hite
Director
Information Technology Architecture and Systems Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Hite:

RE: Draft Report GAO-08-1086, Secure Border Initiative: DHS Needs to Address Significant Risks in Delivering Key Technology Investment (GAO Job Code 310644)

The Department of Homeland Security (DHS) appreciates the opportunity to review and comment on the draft report referenced above that focuses on the technology component (“SBI^{net}”) of the Department’s Secure Border Initiative. The GAO report addresses three broad areas of concern: (1) limited definition of SBI^{net} deployments, capabilities, schedule, and lifecycle management processes; (2) limitations of SBI^{net} requirements development and management efforts; and (3) limitations in key SBI^{net} testing and test management activities.

U.S. Customs and Border Protection (CBP) acknowledges that the GAO report is factually sound. CBP concurs with recommendations 1 through 7 and partially non-concurs with recommendation 8 for Executive Action. The draft report highlights several management and operational challenges that CBP is working to resolve as expeditiously as possible. To address the challenges described in the draft report, CBP has initiated a series of actions to improve both the technical and management processes for SBI^{net}.

Beginning with the DHS’s Deep Dive Review and other internal assessments and continuing through GAO’s review, CBP has identified many of the same concerns as GAO.

On August 19, 2008, CBP met with the DHS Investment Review Board to formally discuss program risk and agree on courses of action to best mitigate this risk. The most significant result of this meeting was DHS’s direction to delay the TUS-1 and AJO-1 deployments into 2009. This recognizes the need to manage the technology risk before the deployment, and also to divert funds intended to be used for these deployments in

Fiscal Year (FY) 2008 to address more urgent vehicle and pedestrian fencing project funding requirements. CBP believes this risk assessment, executive briefings, and discussion not only satisfy the requirements of Recommendations 1 and 2 but also help to ensure that program goals are met.

Following the decision to delay the two deployments, SBI was also directed to provide programmatic documentation to DHS. This comprehensive programmatic documentation will include:

- Acquisition Program Baseline (APB) including:
 - A clear articulation of the overall program scope.
 - Out-year Future Years Homeland Security Program (FYHSP) profile.
 - A description of the program's evolutionary approach, including Key Performance Parameters (KPPs) by Block release.
 - A definition of Block 1, including Common Operating Picture (COP) Release 0.5 usable segment.
 - A Block deployment approach.
 - The Block 1 phased deployment approach.
 - Realistic cost and schedule thresholds for Block 1 including individual phases of deployment within the Block.
 - Establishment of a Key Decision Point (KDP) 2 date.
- Test and Evaluation Master Plan (TEMP)
- Life Cycle Cost Estimate (LCCE)
- Integrated Logistics Sustainment Plan (ILSP)
- Systems Engineering Plan (SEP)
- Revised Operational Requirements Document (ORD) – allocated Block 1 requirements
- SBI*net* Integrated Master Schedule (IMS)
- SBI*net* Operational Capabilities Document

We are confident that this programmatic documentation will satisfy Recommendations 3, 4, 5, and 7. Recommendation 6 is addressed within this document. CBP does not, however, fully concur with Recommendation 8. As noted above, CBP will provide testing requirements and a testing plan that will satisfy most of this recommendation.

The eight recommendations and corrective actions to address them are included below:

Recommendations 1 and 2

To improve DHS's efforts to acquire and implement SBI*net*, as well as to permit meaningful measurement and oversight of and accountability for the program, we recommend that the Secretary of Homeland Security direct the CBP Commissioner to ensure that (1) the risks associated with planned SBI*net* acquisition, development, testing, and deployment activities are immediately assessed, and (2) the results, including proposed alternative courses of action for mitigating them, are provided to the Commissioner and DHS's senior leadership.

RESPONSE:

CBP concurs with Recommendations 1 and 2.

CBP identified and briefed DHS's senior leadership on the risks associated with the planned *SBI*net acquisition, development, testing, and deployment activities. As a result, *SBI*net will develop a detailed program re-plan with supporting program documentation and a *SBI*net Block I APB. It should be noted that DHS and CBP have also begun collaborating on *SBI*net program re-planning alternatives to reduce schedule concurrency (program risk) between system testing and deployment. Proposed alternative courses of action for mitigating them will continue to be briefed to the Commissioner and DHS's senior leadership.

Due Date: December 31, 2008

Recommendation 3

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 when these capabilities are to be deployed and are to be operational.

RESPONSE:

CBP concurs with Recommendation 3.

*SBI*net will develop detailed projections as part of the *SBI*net Block 1 APB that will establish and baseline the specific Block 1 program commitments, including the specific system functional and performance capabilities that are to be deployed to the Tucson and Yuma Border Patrol Sectors. Because of the current re-planning, CBP is now planning to field *SBI*net to the El Paso Sector as part of *SBI*net Block 2, which will likely be delivered over FYs 2011 through 2012.

Due Date: December 31, 2008

Recommendation 4

Finalize and approve an integrated master schedule that reflects the timing and sequencing of the work needed to achieve these commitments.

RESPONSE:

CBP concurs with Recommendation 4.

A finalized and approved integrated master schedule that reflects the timing and sequencing of the work needed will be completed, re-baselined, and included in the *SBI*net Block 1 APB.

Due Date: December 31, 2008

Recommendation 5

Revise and approve versions of the *SBI*net life cycle management approach, including the draft System Engineering Plan and draft Test and Evaluation Management Plan, and in doing so, ensure that these revised and approved versions are consistent with one another, reflect program officials' recently described changes to the engineering and testing approaches, and reflect relevant federal guidance and associated leading practices.

RESPONSE:

CBP concurs with Recommendation 5.

SBI will include in the *SBI*net Block 1 APB a revised *SBI*net life cycle management approach, including a System Engineering Plan and a Test and Evaluation Management Plan (TEMP). SBI will ensure that the approved versions reflect program officials' recently described changes to the engineering and testing approaches, and reflect relevant federal guidance and associated leading practices. The *SBI*net Block I APB will include supporting documentation for key program management processes related to program requirements and performance projections, testing and deployment plans, integrated schedules, cost estimates and risk assessments.

Due Date: December 31, 2008

Recommendation 6

Ensure that the revised and approved life cycle management approach is fully implemented.

RESPONSE:

CBP concurs with Recommendation 6.

*SBI*net will develop a quality management program to ensure that the revised and approved life cycle management approach is fully implemented.

Due Date: December 31, 2008

Recommendation 7

Implement key requirements development and management practices to include (1) baselining requirements before system design and development efforts begin; (2) analyzing requirements prior to being baselined to ensure that they are complete, achievable, and verifiable; and (3) tracing requirements to higher-level requirements, lower-level requirements, and test cases.

RESPONSE:

CBP concurs with Recommendation 7.

CBP understands and will comply with GAO's recommendation for following a disciplined set of activities for the analysis and documentation (i.e., "baselining") of key system requirements and the definition and documentation of detailed performance specifications and test plans underpinning the key system requirements. The *SBI*net Block I APB will be based on completed system requirements, system design specifications, and detailed test plans. Also in conjunction with the *SBI*net Block I Qualification Test Readiness Review, CBP will complete its ongoing effort to update the appropriate databases for tracing all of these detailed requirements (i.e., the DOORS database).

While CBP officials concur with this recommendation, CBP officials would like to note that *SBI*net personnel believe that rather than a sequential "heel-to-toe" approach for these efforts (i.e. identifying baseline requirements before beginning design and test) *SBI*net is employing a "spiral" approach of iterative design-prototype-test-learn cycles. This spiral development approach provides for an initial definition of requirements (under formal configuration control), and then a period of development and testing to gain user feedback and engineering confidence with initial (sometimes draft) designs. Final requirements, as well as final designs, are worked together and often in parallel. The initial test spirals also help to complete detailed test plans and procedures needed for final qualification and acceptance testing.

Due Date: December 31, 2008

Recommendation 8

Implement key test management practices to include (1) developing and documenting test plans prior to the start of testing; (2) conducting appropriate component level testing prior to integrating system components; and (3) approving a test management strategy that, at a minimum, includes a relevant testing schedule, establishes accountability for testing activities by clearly defining testing roles and responsibilities, and includes sufficient detail to allow for testing and oversight activities to be clearly understood and communicated to test stakeholders.

RESPONSE:

CBP partially non-concurs with Recommendation 8.

This partial non-concurrence results from the recommendation language requiring CBP to "Implement key test management practices to include... (2) conducting appropriate component level testing prior to integrating system components..."

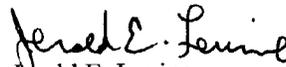
In general, CBP understands and will comply with GAO's recommendation for following a disciplined set of activities for planning, executing, and reporting *SBI*net program testing. While CBP presented to GAO significant progress in maturing *SBI*net testing strategies and plans, to include the hierarchical approach for System Integration Tests, System Qualification Tests, and System Acceptance Tests, CBP acknowledges program management documentation is lagging. CBP will update the *SBI*net Block I APB, which will be based on improved test plans and system test progress to-date. Additionally, CBP will provide an updated TEMP with the *SBI*net Block I APB to highlight specific testing roles, responsibilities, and those parties accountable for the revised test program. Moreover, this TEMP is to be signed by the DHS principal office for *SBI*net test oversight (DHS Science and Technology Directorate).

Regarding "appropriate" component-level testing, the *SBI*net approach provides for disciplined, hierarchical testing at the hardware/software component level, integrated component level, and ultimately at the integrated system level, in the laboratory as well as in operationally representative field conditions. For component-level testing, *SBI*net leadership believes the current test strategy provides the appropriate degree of technical confidence for commercial off the shelf (COTS) components, as evidenced by either Certificates of Conformance from the Original Equipment Manufacturer, test documentation from independent government laboratories, or through Boeing component/integration level testing. *SBI*net believes this approach is consistent with COTS intensive program best practices and avoids the added cost of duplicative component level testing with little added utility. Notwithstanding the differences between the GAO recommendation and *SBI*net implementation, *SBI*net will continue to improve and update program documentation that is comprehensive, consistent, and keeps stakeholders abreast of all activities.

Due Date: December 31, 2008

CBP conducted a sensitivity review of the draft report and did not identify any information that would require a "For Official Use Only" designation. Technical comments have been provided under separate cover and should help clarify particular statements prior to finalizing the report.

Sincerely,



Jerald E. Levine

Director

Departmental GAO/OIG Liaison Office

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Randolph C. Hite, (202) 512-3439 or hiter@gao.gov

Staff Acknowledgments

In addition to the contact named above, Deborah Davis (Assistant Director), Carl Barden, Neil Doherty, Lee McCracken, Jamelyn Payan, Karl Seifert, Sushmita Srikanth, Karen Talley, and Merry Woo made key contributions to this report.

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, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

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