United States Government Accountability Office

GAO

Report to Congressional Requesters

May 2010

SECURE BORDER INITIATIVE

DHS Needs to Reconsider Its Proposed Investment in Key Technology Program

GAO-10-340

May 2010

SECURE BORDER INITIATIVE

DHS Needs to Reconsider Its Proposed Investment in Key Technology Program

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-340, a report to congressional requesters

Why GAO Did This Study

The technology component of the Department of Homeland Security's (DHS) Secure Border Initiative (SBI), referred to as SBI*net*, is to put observing systems along our nation's borders and provide Border Patrol command centers with the imagery and related tools and information needed in deciding whether to deploy agents. SBI*net* is being acquired and deployed in incremental blocks of capability, with the first block to cost about $1.3 billion. Because of the program's importance, size, and challenges, GAO was asked to, among other things, determine the extent to which DHS has (1) defined the scope of its proposed SBI*net* solution, (2) developed a reliable schedule for this solution, (3) demonstrated the cost-effectiveness of this solution, and (4) acquired the solution using key management processes. To do this, GAO compared key program documentation to relevant guidance and industry practices.

What GAO Recommends

GAO is making recommendations to DHS aimed at (1) limiting near-term investment in the first incremental block of SBI*net*, (2) economically justifying any longer-term investment in SBI*net*, and (3) improving key program management disciplines. DHS agreed with 10 of GAO's 12 recommendations, and partially agreed with the other 2. For all of the recommendations, DHS also described planned and ongoing actions to address them.

View GAO-10-340 or key components.
For more information, contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov.

What GAO Found

DHS has defined the scope of the first incremental block of SBI*net* capabilities; however, these capabilities have continued to shrink from what the department previously committed to deliver. For example, the geographical "footprint" of the initially deployed capability has been reduced from three border sectors spanning about 655 miles to two sectors spanning about 387 miles. Further, the stringency of the performance capabilities has been relaxed, to the point that, for example, system performance will be deemed acceptable if it identifies less than 50 percent of items of interest that cross the border. The result is a system that is unlikely to live up to expectations.

DHS has not developed a reliable integrated master schedule for delivering the first block of SBI*net*. Specifically, the schedule does not sufficiently comply with seven of nine key practices that relevant guidance states are important to having a reliable schedule. For example, the schedule does not adequately capture all necessary activities, assign resources to them, and reflect schedule risks. As a result, it is unclear when the first block will be completed, and continued delays are likely.

DHS has also not demonstrated the cost-effectiveness of this first system block. In particular, it has not reliably estimated the costs of this block over its entire life cycle. To do so requires DHS to ensure that the estimate meets key practices that relevant guidance states are important to having an estimate that is comprehensive, well-documented, accurate, and credible. However, DHS's cost estimate for the initial block does not sufficiently possess any of these characteristics. Further, DHS has yet to identify expected benefits from the initial block, whether quantitative or qualitative, and analyze them relative to costs. As a result, it does not know whether its planned investment will produce mission value commensurate with costs.

DHS has also not acquired the initial SBI*net* block in accordance with key life cycle management processes. While processes associated with, among other things, requirements development and management and risk management, have been adequately defined, they have not been adequately implemented. For example, key risks have not been captured in the risk management repository and thus have not been proactively mitigated. As a result, DHS is at increased risk of delivering a system that does not perform as intended.

SBI*net*'s decreasing scope, uncertain timing, unclear value proposition, and limited life cycle management discipline and rigor are due to a range of factors, including limitations in both defined requirements and the capabilities of commercially available system components, as well as the need to address competing program priorities, such as meeting aggressive system deployment milestones. As a result, it remains unclear whether the department's pursuit of SBI*net* is a cost effective course of action, and if it is, that it will produce expected results on time and within budget.

Contents

Tables

Figures

Abbreviations

AJO-1	Ajo Border Patrol Station
CBP	Customs and Border Protection
CDR	Critical Design Review
CMMI	Capability Maturity Model Integration
COP	common operating picture
COTS	commercial off-the-shelf
C3I	command, control, communications, and intelligence
DHS	Department of Homeland Security
DOORS	Dynamic Object-Oriented Requirements System
DT&E	developmental test and evaluation
EVM	earned value management
IMP	integrated master plan
IT	information technology
NOC/SOC	Network Operations Center/Security Operations Center
OMB	Office of Management and Budget
OT&E	operational test and evaluation
SEP	Systems Engineering Plan
SBI	Secure Border Initiative
SBI*net*	Secure Border Initiative Network
SEI	Software Engineering Institute
SPO	SBI*net* System Program Office
TEMP	Test and Evaluation Master Plan
TUS-1	Tucson Border Patrol Station
WBS	work breakdown structure

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

May 5, 2010

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

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

The Honorable Mike Rogers
Ranking Member
Subcommittee on Emergency Communications,
Preparedness, and Response
Committee on Homeland Security
House of Representatives

Securing the 6,000 miles of international borders that the contiguous United States shares with Canada and Mexico is a challenge and a mission imperative to the Department of Homeland Security (DHS). Although hundreds of thousands of illegal aliens are prevented from entering the country each year, many more are not detected. To enhance border security and reduce illegal immigration, DHS launched its multiyear, multibillion dollar Secure Border Initiative (SBI) program in November 2005. Through SBI, DHS intends to enhance surveillance technologies, raise staffing levels, increase domestic enforcement of immigration laws, and improve the physical infrastructure along the nation's borders.

Within SBI, Secure Border Initiative Network (SBI*net*) is a multibillion dollar program that includes the acquisition, development, integration, deployment, and operation and maintenance of surveillance technologies to create a "virtual fence" along the border, as well as command, control, communications, and intelligence (C3I) technologies to create a picture of the border in command centers and vehicles. Managed by DHS's Customs and Border Protection (CBP), SBI*net* is intended to strengthen the ability

of CBP to detect, identify, classify, track, and respond to illegal breaches at and between land ports of entry.[1]

In September 2008, we reported that SBI*net* was at risk because of a number of acquisition management weaknesses, and we made recommendations to address them that DHS largely agreed with and committed to addressing.[2] Because of the importance, high cost, and challenges facing SBI*net*, you subsequently asked us to continue to review DHS's management of SBI*net*. As agreed, our objectives were to determine the extent to which DHS has (1) defined the scope of its proposed system solution, (2) developed a reliable schedule for delivering this solution, (3) demonstrated the cost-effectiveness of this solution, (4) acquired this solution in accordance with key life cycle management processes, and (5) addressed our recent recommendations.

To accomplish our objectives, we largely focused on the first increment of SBI*net* known as Block 1. In doing so, we reviewed key program documentation, including guidance, plans, schedules, cost estimates, and artifacts related to system life cycle events, requirements, risks, and testing. We also analyzed a random probability sample of requirements and their related verification methods. In addition, we interviewed program officials about SBI*net* cost and schedule estimates, program commitments, the development and implementation of the SBI*net* system life cycle approach, requirements development and management, test management, and risk management. We then compared this information to relevant federal guidance, leading industry practices, and the recommendations in our September 2008 report on SBI*net* to identify any deviations and interviewed program officials as to the reasons for any deviations. To assess the reliability of the data that we relied on to support the findings in the report, we reviewed relevant program documentation to substantiate evidence obtained through interviews with knowledgeable agency officials, where available. We determined that the data used in this report are sufficiently reliable. We have also made appropriate attribution indicating the sources of the data used.

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

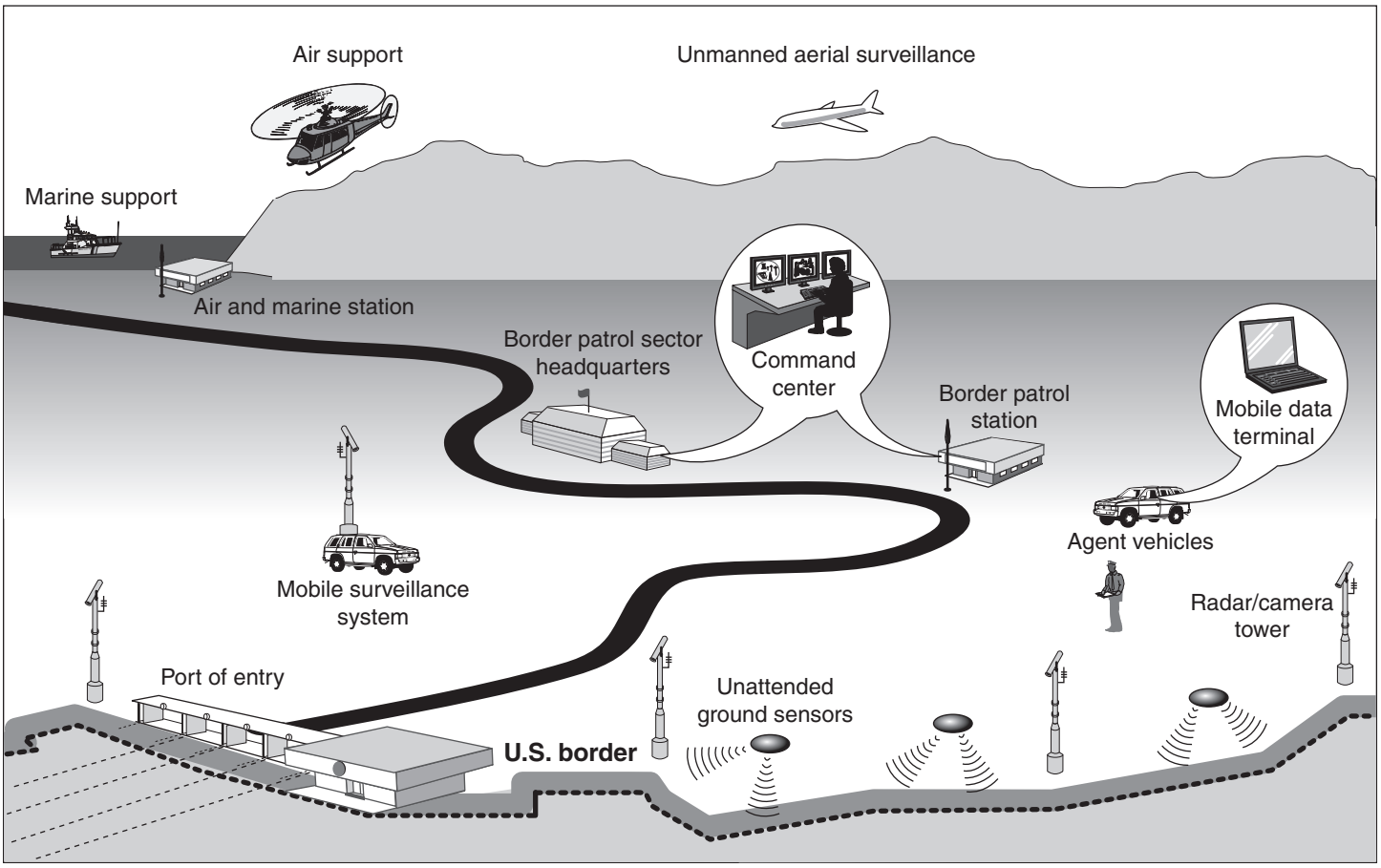
[2]GAO, *Secure Border Initiative: DHS Needs to Address Significant Risks in Delivering Key Technology Investment*, GAO-08-1086 (Washington, D.C.: Sept. 22, 2008).

We conducted this performance audit from December 2008 to May 2010 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 in appendix I.

Background

SBI*net* includes the acquisition, development, integration, deployment, and operations and maintenance of a mix of surveillance technologies, such as cameras, radars, sensors, and 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 land ports of entry. Longer term, SBI*net* is to address requirements of CBP's Office of Field Operations, which controls vehicle and pedestrian traffic at the ports of entry, and its Office of Air and Marine Operations, which operates helicopters, fixed-wing aircraft, and marine vessels used in securing the borders. (See fig. 1 for the potential long-term SBI*net* concept of operations.)

Figure 1: Potential Long-Term SBI*net* Concept of Operations



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

Surveillance technologies are to include a variety of sensor systems. Specifically, unattended ground sensors are to be used to detect heat and vibrations associated with foot traffic and metal associated with vehicles. Radar mounted on fixed and mobile towers is to detect movement, and cameras on fixed and mobile towers are to be used by operators to identify and classify items of interest detected and tracked by ground sensors and radar. Aerial assets are also to be used to provide video and infrared imaging to enhance tracking targets. These technologies are generally to be acquired through the purchase of commercial off-the-shelf (COTS) products.

C3I technologies (software and hardware) are to produce a common operating picture (COP)—a uniform presentation of activities within specific areas along the border. Together, the sensors, radar, and cameras are to gather information along the border and transmit this information to COP terminals located in command centers and agents' vehicles, which in turn are to assemble it to provide CBP agents with border situational awareness. Among other things, COP hardware and software are to allow agents to (1) view data from radar 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.

Overview of SBI*net* Management Structure, Acquisition Approach, and Status

To increase border security and decrease illegal immigration, DHS launched SBI more than 4 years ago after canceling its America's Shield Initiative program.[3] Since fiscal year 2006, DHS has received about $4.4 billion in appropriations for SBI, including about $2.5 billion for physical fencing and related infrastructure, about $1.5 billion for virtual fencing (surveillance systems) and related technical infrastructure (towers), and about $300 million for program management.[4] The SBI Program Executive Office, which is organizationally within CBP, is responsible for managing key acquisition functions associated with SBI*net*, including prime contractor tracking and oversight.[5] It is organized into four components: SBI*net* System Program Office (referred to as the SPO in this report), Systems Engineering, Business Management, and Operational Integration.[6] As of December 31, 2009, the SBI Program Executive Office was staffed with 188 people—87 government employees, 78 contractor staff, and 13 detailees.

In September 2006, CBP awarded a 3-year prime contract to the Boeing Company, with three additional 1-year options for designing, producing,

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

[4]The remaining $126 million was for upgrading the supporting CBP telecommunications links.

[5]In addition to the SBI Program Office, the SBI Acquisition Office is responsible for performing contract administration activities.

[6]The physical infrastructure (e.g., physical fencing) portion of SBI is managed on a day-to-day basis by CBP's Office of Finance Facilities Management and Engineering division.

testing, deploying, and sustaining SBI. In 2009, CBP exercised the first option year. Under this contract, CBP has issued 10 task orders that relate to SBI*net*, covering for example, COP design and development, system deployment, and system maintenance and logistics support. As of December 2009, 4 of the 10 task orders had been completed and 6 were ongoing. (See table 1 for a summary of the SBI*net* task orders.)

Table 1: Summary of SBI*net* Task Orders as of December 2009

Dollars in millions

Task order	Description	Period of performance	Approximate contract value	Approximate contract obligation	Contract type
Program Management	Mission engineering, facilities and infrastructure, systems engineering, test and evaluation, and program management services.	Sep. 2006-Apr. 2008 (completed)	$146.9	$146.9	Cost-plus-fixed-fee[a]
Project 28	Prototype along 28 miles of the border in the Tucson Sector.	Oct. 2006-Feb. 2008 (completed)	$20.7	$20.7	Firm-fixed-price
Project 28 Contractor Maintenance Logistics and Support	Project 28 operational maintenance and logistics support.	Dec. 2007-Dec. 2009 (completed)	$10.6	$10.6	Cost-plus-fixed-fee
Design for Buffalo Sector	SBI*net* design of remote video surveillance system capability for the Buffalo Sector.	Feb. 2009-July 2009 (completed)	$0.6	$0.6	Firm-fixed-price[b]
Design	Design of deployment solution, environmental clearance support, and other location-related work for the Tucson Sector.	Aug. 2007-July 2010 (ongoing)	$115.0	$115.0	Cost-plus-fixed-fee
Command, Control, Communications, and Intelligence (C3I) Common Operating Picture (COP)	Design, development, demonstration, and operations and maintenance of a functional C3I/COP system.	Dec. 2007-Feb. 2010 (ongoing)	$73.0	$71.0	Cost-plus-award-fee/cost-plus-fixed-fee/firm-fixed-price[c]
System	Program management and system engineering activities required to integrate all task orders.	Apr. 2008-Mar. 2010 (ongoing)	$205.8	$200.8	Cost-plus-award-fee
Arizona Deployment	Deployment to two sites covering approximately 53 miles of the southwest border in the Tucson Sector	June 2008-May 2010 (ongoing)	$115.0	$90.5	Cost-plus-incentive-fee/cost-plus-award-fee[d]
Integrated Logistics Support	Maintenance logistics and operational support.	Aug. 2008-Sep. 2010 (ongoing)	$61.6	$61.6	Cost-plus-fixed-fee[e]
Northern Border Project	Design, installation, and deployment of surveillance capabilities in the Detroit and Buffalo Sectors.	Mar. 2009-Mar. 2010 (ongoing)	$22.4	$20.9	Fixed-price[f]

Source: GAO analysis of DHS data.

Note: *Fixed-price* types of contracts provide for a firm price or, in appropriate cases, an adjustable price; *firm-fixed-price* contracts provide for a price not subject to adjustment on the basis of the contractor's experience in performing the contract; *cost-plus-incentive-fee* contracts provide for the reimbursement of allowable costs plus an initially negotiated fee, to be adjusted later based on the relationship of total allowable costs to total target costs; *cost-plus-award-fee* contracts provide for the reimbursement of allowable costs plus a base fee fixed at the contract's inception (which may be zero) and an award amount that the government determines to be sufficient to motivate excellence in performance; *cost-plus-fixed-fee* contracts provide for the reimbursement of allowable costs plus a negotiated fee fixed at the inception of the contract.

[a]The initial contract type of the task order was a cost-plus-award-fee. A final award fee determination did not take place because of scope and schedule changes. In lieu of the final award fee determination, the contract type was changed to a cost-plus-fixed-fee.

[b]The travel component of the task order is cost reimbursable.

[c]The initial contract type of the task order was cost-plus-award-fee. On July 31, 2009, additional development work was definitized as a cost-plus-fixed-fee structure. Further, on September 30, 2009, the software operations and maintenance component of the task order was changed to a firm-fixed-price structure.

[d]The initial contract type of the task order was a cost-plus-incentive-fee. On November 20, 2009, the performance and schedule incentives component of the task order was changed to a cost-plus-award-fee. The cost incentives component remains a cost-plus-incentive-fee structure.

[e]The initial contract type of the task order was cost-plus-incentive-fee. On November 6, 2009, future work under the task order was changed to a cost-plus-fixed-fee structure.

[f]The travel component of the task order is cost reimbursable.

One of the completed task orders is for an effort known as Project 28, which is a prototype system that covers 28 miles of the border in CBP's Tucson Sector[7] in Arizona, and has been operating since February 2008. However, its completion took 8 months longer than planned because of problems in integrating system components (e.g., cameras and radars) with the COP software. As we have reported,[8] these problems were attributable to, among other things, limitations in requirements development and contractor oversight.

Through the task orders, CBP's strategy is to deliver SBI*net* capabilities incrementally. To accomplish this, the SPO has adopted an evolutionary system life cycle management approach in which system capabilities are to be delivered to designated locations in a series of discrete subsets of

[7]CBP 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.

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

system functional and performance capabilities that are referred to as blocks. The first block, which has been designated as Block 1, includes the purchase of commercially available surveillance systems, development of customized COP systems and software, and use of existing CBP communications and network capabilities. Such an incremental approach is a recognized best practice for acquiring large-scale, complex systems because it allows users access to new capabilities and tools sooner, and thus permits both their early operational use and evaluation. Subsequent increments of SBI*net* capabilities are to be delivered based on feedback and unmet requirements, as well as the availability of new technologies.

In general, the SBI*net* life cycle management approach consists of four primary work flow activities: (1) Planning Activity, (2) System Block Activity, (3) Project Laydown Activity, and (4) Sustainment Activity. During the Planning Activity, the most critical user needs are to be identified and balanced against what is affordable and technologically available. The outcome of this process is to be a set of capability requirements that are to be acquired, developed, and deployed as a specific block. This set of capabilities, once agreed to by all stakeholders, is then passed to the System Block Activity, during which the baseline system solution to be fielded is designed and built. Also as part of this activity, the verification steps are to be conducted on the individual system components and the integrated system solution to ensure that they meet defined requirements. The Project Laydown Activity is performed to configure the block solution to a specific geographic area's unique operational characteristics. This activity involves assessing the unique threats, terrain, and environmental concerns associated with a particular area, incorporating these needs into the system configuration to be deployed to that area, obtaining any needed environmental permits, and constructing the infrastructure and installing the configured system. It also involves test and evaluation activities, including system acceptance testing, to verify that the installed block system was built as designed. The final activity, Sustainment, is focused on the operations and maintenance of the deployed block solution and supporting the user community.

Associated with each of these activities are various milestone or gate reviews. For example, a key review for the System Block Activity is the Critical Design Review (CDR). At this review, the block design and requirements are baselined and formally controlled to approve and track any changes. Among other things, this review is to verify that the block solution will meet the stated requirements within the program's cost and schedule commitments. An important review conducted during the Project Laydown Activity is the Deployment Design Review. At this review,

information such as the status of environmental reviews and land acquisitions for a specific geographic area is assessed, and the location-specific system configuration is determined. The Deployment Readiness Review is another key event during this activity. During this review, readiness to begin site preparation and construction is assessed.

In addition to the four above described workflow activities are various key life cycle management processes, such as requirements development and management, risk management, and test management.

Requirements development and management, among other things, involves defining and aligning a hierarchy of five types of SBI*net* requirements. These five types begin with high-level operational requirements and are followed by increasingly more detailed lower-level requirements, to include system, component, C3I/COP software, and design requirements. To help it manage the requirements, the SPO relies on Boeing's use of a database known as the Dynamic Object-Oriented Requirements System (DOORS). The various types of SBI*net* requirements are described in table 2.

Table 2: SBI*net* Requirements Types

Type	Description
Operational requirements	Describe the operational capabilities that the resulting system must satisfy, and can be viewed as user requirements.
System requirements	Describe the system performance, functional, and nonfunctional characteristics, and provide the basis for system design, development, integration, verification, and deployment.
Component requirements	Describe required features of various surveillance components (e.g., cameras and radars), and infrastructure (e.g., communications).
C3I/COP requirements	Describe the functionality and capability of the COP software, such as allowing the user to control and view information from the sensors.
Design requirements	Describe the operational, behavioral, and physical characteristics of hardware and software interfaces.

Source: GAO analysis of DHS data.

Risk management entails taking proactive steps to identify and mitigate potential problems before they become actual problems. The SPO has defined a "risk" to be an uncertain event or condition that, if it occurs, will have a negative effect on at least one program objective, such as schedule,

cost, scope, or technical performance. The SPO has defined an "issue" as a risk that has been realized (i.e., a negative event or condition that currently exists or has a 100 percent future certainty of occurring). According to SBI*net*'s risk management process, anyone involved in the program can identify a risk. Identified risks are submitted to the Risk Management Team, which includes both the SPO Risk Manager and Boeing Risk Manager, for preliminary review. If approved for further consideration, the risk is entered into the Boeing-owned risk database, which is accessible by SPO and Boeing officials. These risks are subsequently reviewed by the Joint Risk Review Board, which is composed of approximately 20 SPO and Boeing officials. If a risk is approved, it is to be assigned an owner who will be responsible for managing its mitigation.

Test management involves planning, conducting, documenting, and reporting on a series of test events that first focus on the performance of individual system components, then on the performance of integrated system components, followed by system-level tests that focus on whether the system (or major system increments) are acceptable and operationally suitable. For SBI*net*, the program's formal test events fall into two major phases: developmental test and evaluation (DT&E) and operational test and evaluation (OT&E). DT&E is to verify and validate the systems engineering process and provide confidence that the system design solution satisfies the desired capabilities. It consists of four test events—integration testing, component qualification testing, system qualification testing, and system acceptance testing. OT&E is to ensure that the system is effective and suitable in its operational environment with respect to key considerations, including reliability, availability, compatibility, and maintainability. SBI*net* defines three operational testing events—User Assessment, Operational Test, and Follow-on Operational Test and Evaluation. (See table 3 for each test event's purpose, responsible parties, and location.)

Table 3: Overview of Formal Test Events

Test	Purpose	Party responsible	Location
DT&E events			
Integration testing	Demonstrate interoperability among system components, and ensure the proper functioning of individual component hardware and software interfaces.	Contractor performs with SPO witnesses	Laboratory and field test site
Component qualification testing	Verify the functional performance of individual components against component requirements.	Contractor performs with SPO witnesses	Laboratory and field test site
System qualification testing	Verify that the system design satisfies system-level requirements.	Contractor performs with SPO witnesses	Field test site and deployment site
System acceptance testing	Verify that the deployed system is built as designed and performs as predicted in the deployed environment.	Contractor performs with SPO witnesses	Deployment site
OT&E events			
User assessment	Identify potential operational problems and progress toward meeting requirements using the version of the system tested during system qualification testing.	CBP, SPO, and U.S. Army Independent Test & Evaluation Team performs	Field test site
Operational test	Determine whether the system meets defined key performance parameters in its operational environment.	CBP and U.S. Army Independent Test & Evaluation Team performs	Deployment site
Follow-on operational test and evaluation	Refine estimates made during OT&E, evaluate changes, and re-evaluate the system to ensure that it continues to meet operational needs.	U.S. Army Independent Test & Evaluation Team performs	Deployment site

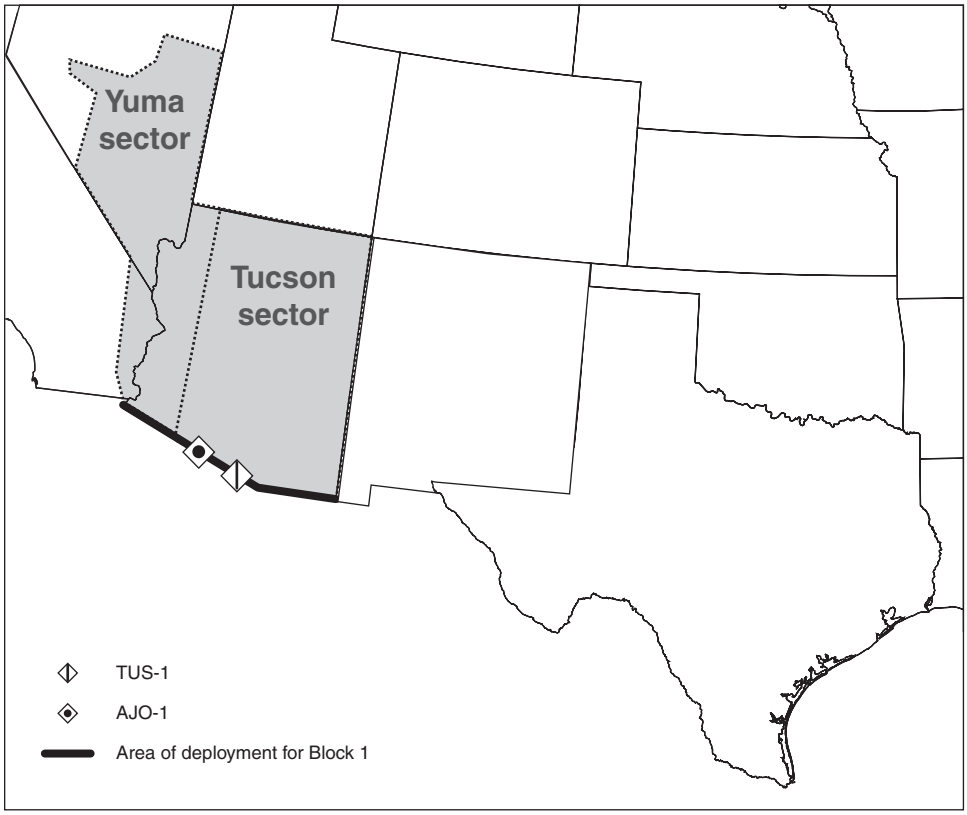
Source: GAO analysis of DHS data.

As of December 2009, the program was in the Project Laydown Activity. Specifically, the SBI*net* CDR was completed in October 2008, and the Block 1 design has been configured and is being tested and readied for deployment to the Tucson Border Patrol Station (TUS-1), and then to the Ajo Border Patrol Station (AJO-1), both of which are located in the CBP's Tucson Sector of the southwest border. More specifically, the Deployment Design Review covering both TUS-1 and AJO-1 was completed in June 2007, the TUS-1 Deployment Readiness Review was completed in April 2009, and the AJO-1 Deployment Readiness Review was completed in December 2009. Together, these two deployments are to cover 53 miles of the 1,989-mile-long southern border[9] (see fig. 2). Once a deployed configuration has been accepted and is operational, the program will be in

[9]The area that will be covered by TUS-1 covers 23 of the 28 miles associated with Project 28. According to the SPO, the Project 28 capabilities (surveillance systems and COP) will be replaced with Block 1 capabilities as part of the TUS-1 deployment.

the Sustainment Activity. As of November 2009, program documentation showed that TUS-1 and AJO-1 were to be accepted in January and July 2010, respectively. However, the SBI Executive Director told us in December 2009 that these and other SBI*net* scheduled milestones are currently being re-evaluated. As of February 2010, TUS-1 and AJO-1 were proposed to be accepted in September 2010 and November 2010, respectively. However, this proposed schedule has yet to be approved by CBP.

Figure 2: Map of Block 1 Deployments



Sources: GAO analysis of DHS data, MapArt (map).

GAO Has Previously Reported on Numerous SBI*net* Management Weaknesses and Risks

Since 2007, we have identified a range of management weaknesses and risks facing SBI*net* and we have made a number of recommendations to address them that DHS has largely agreed with and, to varying degrees, taken actions to address. For example, in February 2007, we reported that DHS had not fully defined activities, milestones, and costs for

implementing the program; demonstrated how program activities would further the strategic goals and objectives of SBI; and reported on the costs incurred, activities, and progress made by the program in obtaining operational control of the border.[10] Further, we reported that the program's schedule contained a high level of concurrency among related tasks and activities, which introduced considerable risk. Accordingly, we recommended that DHS define explicit and measurable commitments relative to, among other things, program capabilities, schedules, and costs, and re-examine the level of concurrency in the schedule and adjust the acquisition strategy appropriately. We are currently reviewing DHS's Fiscal Year 2010 SBI Expenditure Plan to, among other things, determine the status of DHS's actions to address these recommendations.

In October 2007, we testified that DHS had fallen behind in implementing Project 28 due to software integration problems, although program officials stated at that time that Boeing was making progress in correcting the problems.[11] Shortly thereafter, we testified that while DHS had accepted Project 28, it did not fully meet expectations.[12] To benefit from this experience, program officials stated that they identified a number of lessons learned, including the need to increase input from Border Patrol agents and other users in SBI*net* design and development.

In September 2008, we reported that important aspects of SBI*net* were ambiguous and in a continued state of flux, making it unclear and uncertain what technological capabilities were to be delivered when.[13] We concluded that the absence of clarity and stability in key aspects of SBI*net* impaired the ability of Congress to oversee the program and hold DHS accountable for results, and hampered DHS's ability to measure program performance. As a result, we recommended that the SPO establish and baseline the specific program commitments, including the specific system functional and performance capabilities that are to be deployed, and when they were to be deployed.

[10]GAO, *Secure Border Initiative: SBInet Expenditure Plan Needs to Better Support Oversight and Accountability*, GAO-07-309 (Washington, D.C.: Feb. 15, 2007).

[11]GAO-08-131T.

[12]GAO-08-508T.

[13]GAO-08-1086.

Also, we reported that the SPO had not effectively performed key requirements definition and management practices. For example, it had not ensured that different levels of requirements were properly aligned, as evidenced by our 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 were derived from them. As a result of these limitations, we concluded that the risk of SBI*net* not meeting mission needs and performing as intended was increased, as were the chances of the program needing expensive and time-consuming system rework. We recommended that the SPO 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 that they are complete, achievable, and verifiable; and (3) tracing requirements to higher-level requirements, lower-level requirements, and test cases.

We also reported that SBI*net* testing was not being effectively managed. For example, the SPO had not tested the individual system components to be deployed to the initial deployment locations, even though the contractor had initiated integration testing of these components with other system components and subsystems. Further, while a test management strategy was drafted, it had not been finalized and approved, and it did 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. We concluded that without a structured and disciplined approach to testing, the risk that SBI*net* would not satisfy user needs and operational requirements, thus requiring system rework, was increased. We recommended that the SPO (1) develop and document test practices prior to the start of testing; (2) conduct appropriate component-level testing prior to integrating system components; and (3) approve 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.

In light of these weaknesses and risks, we further recommended that (1) the risks associated with planned SBI*net* acquisition, development,

testing, and deployment activities be immediately assessed and (2) the results, including proposed alternative courses of action for mitigating the risks, be provided to the CBP Commissioner and DHS's senior leadership, as well as to the department's congressional authorization and appropriations committees. DHS agreed with all but one of the recommendations in our September 2008 report. The status of DHS's efforts to implement these recommendations is summarized later in this report and discussed in detail in appendix III.

In September 2009, we reported that SBI*net* had continued to experience delays.[14] For example, deployment to the entire southwest border had slipped from early 2009 to 2016, and final acceptance of TUS-1 and AJO-1 had slipped from November 2009 and March 2010 to December 2009 and June 2010, respectively. We did not make additional SBI*net* recommendations at that time.

Most recently, we reported in January 2010 that SBI*net* testing was not being effectively managed.[15] Specifically, while DHS's approach to testing appropriately consisted of a series of progressively expansive developmental and operational test events, the test plans, cases, and procedures for the most recent test events were not defined in accordance with important elements of relevant guidance. For example, none of the plans adequately described testing risks and only two of the plans included quality assurance procedures for making changes to test plans during their execution. Further, a relatively small percentage of test cases for these events described the test inputs and the test environment (e.g., facilities and personnel to be used), both of which are essential to effective testing.

In addition, a large percentage of the test cases for these events were changed extemporaneously during execution. While some of the changes were minor, others were more significant, such as re-writing entire procedures and changing the mapping of requirements to test cases. Moreover, these changes to procedures were not made in accordance with documented quality assurance processes, but rather were based on an undocumented understanding that program officials said they established

[14]GAO, *Secure Border Initiative: Technology Deployment Delays Persist and the Impact of Border Fencing Has Not Been Addressed*, GAO-09-896 (Washington, D.C.: Sept. 9, 2009).

[15]GAO, *Secure Border Initiative: DHS Needs to Address Testing and Performance Limitations That Place Key Technology Program at Risk*, GAO-10-158 (Washington, D.C.: Jan. 29, 2010).

with the contractor. Compounding the number and significance of changes were questions raised by the SPO and a support contractor about the appropriateness of some changes. For example, the SPO wrote to the prime contractor that changes made to system qualification test cases and procedures appeared to be designed to pass the test instead of being designed to qualify the system.

Further, we reported that from March 2008 through July 2009, that about 1,300 SBI*net* defects had been found, with the number of new defects identified during this time generally increasing faster than the number being fixed—a trend that is not indicative of a system that is maturing and ready for deployment. While the full magnitude of these unresolved defects was unclear because the majority were not assigned a priority for resolution, some of the defects that had been found were significant. Although DHS reported that these defects had been resolved, they had nevertheless caused program delays, and related problems had surfaced that continued to impact the program's schedule. Further, an early user assessment of SBI*net* had raised significant concerns about the performance of key system components and the system's operational suitability.

In light of these weaknesses, we recommended that DHS (1) revise the program's overall test plan to include (a) explicit criteria for assessing the quality of test documentation, including test plans and test cases, and (b) a process for analyzing, prioritizing, and resolving program defects; (2) ensure that test schedules, plans, cases, and procedures are adequately reviewed and approved consistent with the revised test plan; (3) ensure that sufficient time is provided for reviewing and approving test documents prior to beginning a given test event; and (4) triage the full inventory of unresolved system problems, including identified user concerns, and periodically report on their status to CBP and DHS leadership. DHS fully agreed with the last three recommendations and partially agreed with the first.

Block 1 Capabilities, Geographic Coverage, and Performance Standards Continue to Decrease

For Block 1, functional and performance capabilities and the number of geographic locations to which they are to be deployed have continued to decrease. We reported in September 2008 that the capabilities and deployment locations of SBI*net* were decreasing.[16] Since that time, the number of component-level requirements to be deployed to TUS-1 and AJO-1 has decreased by about 32 percent. In addition, the number of sectors that the system is to be deployed to has been reduced from three to two, and the stringency of the system performance measures that the deployed system is to meet has been reduced. According to program officials, the decreases are due to poorly defined requirements and limitations in the capabilities of commercially available system components. The result will be a deployed and operational system that, like Project 28, does not live up to user expectations and provides less mission support than was envisioned.

Functional Capabilities Have Been Reduced

Since our September 2008 report, the number of requirements that Block 1 is to meet has dropped considerably. Specifically, in September 2008, DHS directed the SPO to identify the operational requirements to be allocated to Block 1. In response, 106 operational requirements were established, such as providing border surveillance, facilitating decision support and situational awareness, enabling communications, providing operational status and readiness metrics, and enabling system audits. Of the 106 requirements, 69 were to be included in the initial technology deployments planned for TUS-1 and AJO-1. The remaining 37 were to be addressed in future blocks.

To implement the 69 operational requirements, the SPO developed a system-level requirement specification and 12 component-level requirements specifications.[17] More specifically, as part of CDR, which concluded in October 2008, the 69 operational requirements for TUS-1 and AJO-1 were associated with 97 system-level requirements. Also during CDR, the 97 system-level requirements were associated with 1,286 component-level requirements.

However, between October 2008 and September 2009, the number of component-level requirements was reduced from 1,286 to 880, or by about

[16]GAO-08-1086.

[17]A specification is the written collection of individual requirements for a given hardware component (e.g., camera or radar) or a software subsystem (e.g., COP).

32 percent. First, 281 requirements related to the specifications for three components—communications, network operations, and network security—were eliminated, leaving 1,005 baselined requirements.[18]

Examples of the 281 requirements that were eliminated include the following:

- the failure in a single piece of hardware or software would not affect mission critical functions which include detection and resolution of border incursions;
- the failure of a Network Operations Center/Security Operations Center[19] (NOC/SOC) workstation would not prevent the system from operating; and
- the failure of one network power supply would be compensated for by additional backup power supplies.

In addition, another 125 component-level requirements were granted "waivers" or "deviations,"[20] further reducing the number of Block 1 requirements to be deployed to TUS-1 and AJO-1 to 880 (as of September 2009). For example, the unattended ground sensors were required to differentiate between human, vehicle, and animal targets. However, because the sensors that are to be deployed to TUS-1 and AJO-1 are only able to identify potential vehicles and are not able to differentiate between humans and animals, this requirement was deviated. Similarly, the radar was required to classify targets as humans or vehicles. However, the radar also cannot differentiate between classes of targets (e.g., humans and vehicles). As a result, the requirement in the radar specification was also deviated.

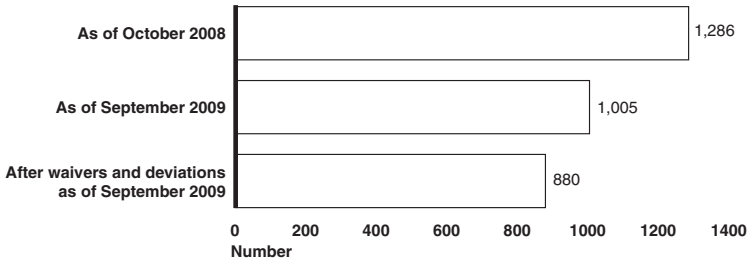
[18]The requirements baseline establishes a set of requirements that have been formally reviewed, agreed upon, and placed under formal change control. The requirements baseline serves as the basis for system design and development.

[19]The NOC monitors SBI*net* equipment with network connections and provides alerts of network events. The SOC protects SBI*net* equipment with network connections from external and internal network-based attacks and provides user authentication services.

[20]According to program documentation, a deviation is a request from the contractor to deliver a product that temporarily departs from a specified requirement, with the expectation that the product will eventually be modified to meet the requirement. A waiver is a request from the contractor to deliver a product that will not meet a specified requirement, but is considered suitable for use as delivered. In the case of a waiver, there is no expectation that the product will ever be changed to meet the requirement.

Figure 3 summarizes the roughly 32 percent drop in requirements that has occurred over the last 15 months.

Figure 3: Illustration of Reduction in Block 1 Requirements



Source: GAO analysis of DHS data.

According to program officials, component requirements were eliminated because they were either poorly written or duplicative of other requirements, or because the capabilities of commercially available products were limited. In addition, they attributed a significant number of eliminated requirements to a decision to not use a Boeing designed and developed network and instead to use an existing DHS network. To the SPO's credit, this decision was made to align SBI*net* with DHS technical standards and to increase the use of COTS products.

Compounding this reduction in Block 1 requirements is the likelihood that further requirements deviations and waivers will be granted based on the results of an early user assessment of the system.[21] According to the July 2009 assessment report, certain SBI*net* components did not meet requirements. For example:

- The daytime cameras were judged to be operationally ineffective over 5 kilometers for identifying humans, while the requirement is that the cameras be usable to 10 kilometers.

[21]The user assessment was conducted from March 27, 2009, to April 3, 2009, in conjunction with personnel from the Johns Hopkins University Applied Physics Laboratory. While the purpose of the assessment was to obtain the users' views of the system's operational effectiveness, and was not designed to be a test of system performance against requirements, the assessment report nonetheless identified instances in which requirements were not met.

- The laser range finder[22] was determined to have an effective range of less than 2 kilometers, while the requirement is for the effective range to be 10 kilometers.

Program officials told us that many of the limitations found during the user assessment were previously known, and corrective actions were already under way or planned for future technology upgrades to address them. However, the officials also stated they plan to issue a waiver or deviation for the camera and the laser range finder to address the two problems discussed above. In addition, they stated that a previously known limitation of the range of the radar will also need to be addressed through a deviation. In this case, the radar is required to have a range of 20 kilometers, but testing shows a maximum range of 10 kilometers.

Geographic Coverage Has Been Reduced

Beyond the requirement reductions, the geographic locations to receive the initial SBI*net* capabilities have also been reduced. As of September 2008, the initial Block 1 deployment was to span three border patrol sectors: Tucson, Yuma, and El Paso—a total of 655 miles. According to program officials, deployment to these three areas was the expressed priority of the Border Patrol due to the high threat levels in these areas. However, the Acquisition Program Baseline,[23] which was drafted in December 2008, states that initial deployment will be to just the Tucson and Yuma Sectors, which will cover only 387 miles.

According to program officials, deployment to the 268 miles of the El Paso Sector was dropped from the initial deployment in anticipation that the sector will instead receive the capabilities slated for the next SBI*net* increment (i.e., build). However, plans for the next increment have not been developed. According to the SBI Executive Director in December 2009, the SPO is re-evaluating where and when future deployments of SBI*net* will occur, and a date for when the revised deployment plans will be available has not been set.

[22]The laser range finder is mounted to the cameras to provide accurate distance data on targets and thereby allows operators to direct Border Patrol agents more effectively.

[23]The Acquisition Program Baseline formally documents a program's critical cost, schedule, and performance parameters, expressed in measurable, quantitative terms that must be met in order to accomplish the program's goals. By tracking and measuring actual program performance against this formal baseline, the program's management is alerted to potential problems, such as cost growth or requirements creep, and has the ability to take early corrective action.

Performance Capabilities Have Decreased

System performance measures define how well a system is to perform certain functions, and thus are important in ensuring that the system meets mission and user needs. According to program documentation, failure to meet a key performance parameter can limit the value of the system and render it unsuccessful. In November 2008, the SPO re-evaluated its existing SBI*net* key performance parameters and determined that SBI*net* must meet three such parameters: (1) the probability of detecting items of interest between the border and the control boundary; (2) the probability of correctly identifying items of interest as human, conveyance, or others; and (3) the operational availability of the system.[24] According to program officials, subject matter experts and CBP staff concluded that these three were critical to determining whether the system successfully meets mission and user needs.

Associated with each parameter is a threshold for acceptable performance. In November 2008, the SPO re-evaluated the thresholds for its three key performance parameters, and it significantly relaxed each of the thresholds:

- The threshold for detecting items of interest dropped from 95 percent to 70 percent.
- The threshold for identifying items of interest declined from 95 percent to 70 percent.[25]
- The threshold for operational availability decreased from 95 to 85 percent.

These threshold reductions significantly lower what constitutes acceptable system performance. For example, the system will meet its detection and identification performance requirements if it identifies 70 percent of the 70 percent of items that it detects, thus producing a 49 percent probability of identifying items of interest that cross the border. Furthermore, the reduction in operational availability means that the time that the system can be unavailable for use has gone from 18.25 days per

[24]System availability is defined as the time the system is operating satisfactorily, expressed as a percentage of time that the system is required to be operational.

[25]The original performance parameter called for the system to be able to "classify" an item of interest as human, vehicle, or animal. Program officials stated that they changed the term to "identify" because "classification" involves determining the level of threat that an identified item of interest presents. For example, a target could be identified as a human, and then classified as a high threat if the person appeared to be carrying a weapon.

year to 54.75 days per year—or from approximately 2.5 weeks to about 7 weeks per year, excluding downtime for planned maintenance.

The SBI Executive Director attributed the performance reductions to program officials' limited understanding of needed operational capabilities at the time the parameters and thresholds were set. The director further stated that once Block 1 has been deployed and Border Patrol personnel gain experience operating it, decisions will be made as to what additional changes to make to the key performance parameters and associated thresholds. Until then, system performance relative to identifying items of interest and operational availability will remain as described above, which program officials agreed fall short of expectations.

A Reliable Schedule for Completing Block 1 Has Not Been Developed

The success of a large-scale system acquisition program like SBI*net* depends in part on having a reliable schedule of when the program's set of work activities and milestone events will occur, how long they will take, and how they are related to one another. Among other things, a reliable schedule provides a road map for systematic execution of a program and the means by which to gauge progress, identify and address potential problems, and promote accountability. Our research has identified nine best practices associated with developing and maintaining a reliable schedule.[26] These are (1) capturing all activities, (2) sequencing all activities, (3) assigning resources to all activities, (4) establishing the duration of all activities, (5) integrating activities horizontally and vertically, (6) establishing the critical path for all activities, (7) identifying reasonable float between activities, (8) conducting a schedule risk analysis, and (9) updating the schedule using logic and durations. To be considered reliable, a schedule should meet all nine practices.

The August 2009 SBI*net* integrated master schedule, which was the most current version available for our review, is not reliable because it substantially complies with only two of the nine key schedule estimating practices and it does not comply with, or only partially or minimally complies with, the remaining seven practices (see table 4 for a summary and app. IV for the detailed results of our analysis of the extent to which the schedule meets each of the nine practices).

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

Table 4: Summary of SBI*net* Integrated Master Schedule Satisfaction of Schedule Estimating Practices

Practice	Met?
Capturing all activities	Minimally
Sequencing all activities	Substantially
Assigning resources to all activities	Minimally
Establishing the duration of all activities	Substantially
Integrating schedule activities horizontally and vertically	Partially
Establishing the critical path for all activities	Partially
Identifying reasonable float between activities	Partially
Conducting a schedule risk analysis	Not
Updating the schedule using logic and durations to determine the dates	Partially

Source: GAO analysis of DHS data.

Note: "Not" means the program provided no evidence that satisfies any portion of the criterion. "Minimally" means the program provided evidence that satisfies less than one-half of the criterion. "Partially" means the program provided evidence that satisfies about one-half of the criterion. "Substantially" means the program provided evidence that satisfies more than one-half of the criterion.

Examples of practices that were either substantially, partially, minimally, or not met are provided below. Without having a reliable schedule, it is unlikely that actual program execution will track to plans, thus increasing the risk of cost, schedule, and performance shortfalls.

- *Capturing all activities:* The schedule does not capture all activities as defined in the program's work breakdown structure[27] or integrated master plan.[28] First, 57 percent of the activities listed in the work breakdown structure (71 of 125) and 67 percent of the activities listed in the integrated master plan (46 of 69) were not in the integrated master schedule. For example, the schedule is missing efforts associated with systems engineering, sensor towers, logistics, system test and evaluation, operations support, and program management. Second, the schedule does not include key activities to be performed by the government. For example, while the schedule shows the final activity in the government

[27]A work breakdown structure defines in detail the hierarchy of work tasks necessary to complete a program's objectives.

[28]An integrated master plan is an event-based hierarchy of program events that must be completed.

process for obtaining an environmental permit in order to construct towers, it does not include the related government activities needed to obtain the permit.

- *Sequencing all activities:* The schedule identifies virtually all of the predecessor and successor activities. Specifically, only 9 of 1,512 activities (less than 1 percent) were missing predecessor links. Further, only 21 of 1,512 activities (about 1 percent) had improper predecessor and successor links. While the number of unlinked activities is very small, not linking a given activity can cause problems because changes to the durations of these activities will not accurately change the dates for related activities. More importantly, 403 of 1,512 activities (about 27 percent) are constrained by "start no earlier than" dates, which is significant because it means that these activities are not allowed to start earlier, even if their respective predecessor activities have been completed.

- *Establishing the critical path for all activities:* The schedule does not reflect a valid critical path[29] for several reasons. First, and as noted above, it is missing government and contractor activities, and is thus not complete. Second, as mentioned above, the schedule is missing some predecessor links, and improperly establishes other predecessor and successor links. Problems with the critical path were recognized by the Defense Contract Management Agency[30] as early as November 2008, when it reported that the contractor could not develop a true critical path that incorporates all program elements.

- *Conducting a schedule risk analysis:* An analysis of the schedule's vulnerability to slippages in the completion of tasks has not been performed. Further, program officials described the schedule as not sufficiently stable to benefit from a risk analysis.

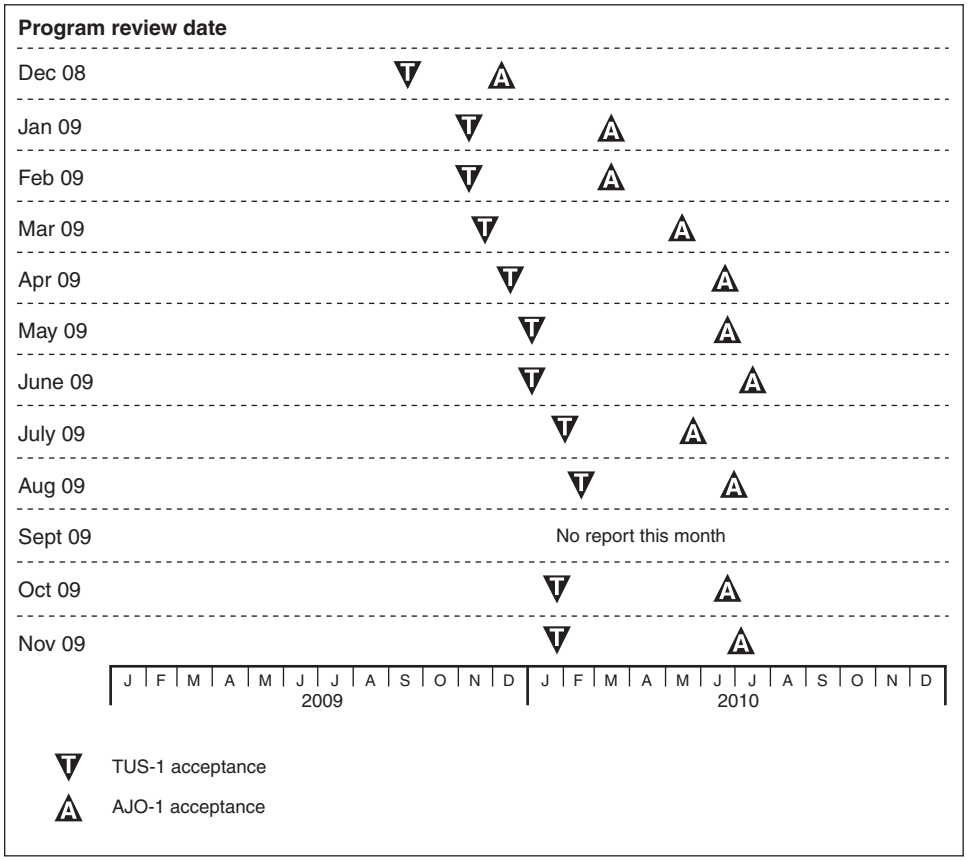
[29]The critical path represents the chain of dependent activities with the longest total duration in the schedule. If any activity on the critical path slips, the entire program will be delayed.

[30]Based on a letter of commitment with CBP, the Defense Contract Management Agency is to provide CBP with contract administration services for SBI*net*, including the identification of issues that could impact Boeing's ability to perform the requirements in the task orders in accordance with established criteria. In this regard, the Defense Contract Management Agency provides the SPO with monthly reports that include an assessment of Boeing's system engineering processes, the current and projected status of operational and technical issues, and the results of ongoing internal audits.

Reasons that these practices were not fully met vary and include the program's use of Boeing to develop and maintain the integrated master schedule, even though Boeing's processes and tools do not allow it to include in the schedule work that it does not have under contract to perform, as well as the constantly changing nature of the work to be performed. Without a reliable schedule that includes all activities necessary to complete Block 1, the SPO cannot accurately determine the amount of time required to complete Block 1, and it does not have an adequate basis for guiding the program's execution and measuring progress, thus reducing the likelihood of meeting the program's completion dates.

Collectively, the weaknesses in meeting the nine key practices for the program's integrated master schedule increase the risk of schedule slippages and related cost overruns and make meaningful measurement and oversight of program status and progress, as well as accountability for results, difficult to achieve. In the case of Block 1, this risk has continued to be realized. For example, the dates presented at the December 2008 to November 2009 monthly program review meetings for government acceptance of Block 1 at TUS-1 and AJO-1 showed a pattern of delays, with TUS-1 and AJO-1 acceptance slipping by 4 months and 7 months, respectively. (See fig. 4.) Moreover, these slipped dates have not been met, and the SBI Executive Director told us in December 2009 that when Block 1 will be accepted and operational continues to change and remains uncertain. As of February 2010, TUS-1 and AJO-1 were proposed to be accepted in September 2010 and November 2010, respectively; however, this proposed schedule has yet to be approved by CBP.

Figure 4: Projected TUS-1 and AJO-1 Acceptance Dates Presented at Monthly Program Review Meetings



Source: GAO analysis of DHS data.

Cost-Effectiveness of Block 1 Has Not Been Demonstrated

As we have previously reported,[31] the decision to invest in any system or major system increment should be based on reliable estimates of costs and meaningful forecasts of quantifiable and qualitative benefits over the system's useful life. For Block 1, DHS does not have a complete and current life cycle cost estimate. Moreover, it has not projected the mission benefits expected to accrue from Block 1 over the same life cycle. According to program officials, it is premature to project such benefits given the uncertainties surrounding the role that Block 1 will ultimately

[31] GAO-09-3SP, 31-36.

play in overall border control operations. Without a meaningful understanding of SBI*net* costs and benefits, DHS lacks an adequate basis for knowing whether the initial system solution on which it plans to spend at least $1.3 billion is cost-effective. Moreover, DHS and congressional decision makers continue to lack a basis for deciding what investment in SBI*net* beyond this initial capability is economically prudent.

Life Cycle Costs Have Not Been Reliably Estimated

A reliable cost estimate is critical to successfully delivering large-scale information technology (IT) systems, like SBI*net*, as well as major system increments, like Block 1. Such an estimate provides the basis for informed investment decision making, realistic budget formulation, meaningful progress measurement, and accountability for results. According to the Office of Management and Budget (OMB),[32] federal agencies must maintain current and well-documented estimates of program costs, and these estimates must encompass the program's full life cycle. Among other things, OMB states that a reliable life cycle cost estimate is critical to the capital planning and investment control process. Without such an estimate, agencies are at increased risk of making poorly informed investment decisions and securing insufficient resources to effectively execute defined program plans and schedules, and thus experiencing program cost, schedule, and performance shortfalls.

Our research has identified a number of practices that form the basis of effective program cost estimating.[33] These practices are aligned with four characteristics of a reliable cost estimate. To be reliable, a cost estimate should possess all four characteristics, each of which is summarized below. (See app. V for the key practices associated with each characteristic, including a description of each practice and our analysis of the extent to which the SBI*net* cost estimate meets each practice.)

- *Comprehensive:* The cost estimate should include all government and contractor costs over the program's full life cycle, from program inception through design, development, deployment, and operation and maintenance

[32]OMB, Circular No. A-11, *Preparation, Submission, and Execution of the Budget* (Washington, D.C., Executive Office of the President, June 2006); Circular No. A-130 Revised, *Management of Federal Information Resources* (Washington, D.C., Executive Office of the President, Nov. 28, 2000); and Capital Programming Guide: Supplement to Circular A-11, Part 7, *Preparation, Submission, and Execution of the Budget* (Washington, D.C., Executive Office of the President, June 2006).

[33]GAO-09-3SP, 8-13.

to retirement. It should also provide sufficient detail to ensure that cost elements are neither omitted nor double counted, and it should document all cost-influencing ground rules and assumptions.

- *Well-documented:* The cost estimate should capture in writing things such as the source and significance of the data used, the calculations performed and their results, and the rationale for choosing a particular estimating method or reference. Moreover, this information should be captured in such a way that the data used to derive the estimate can be traced back to, and verified against, their sources. Finally, the cost estimate should be reviewed and accepted by management to demonstrate confidence in the estimating process and the estimate.

- *Accurate:* The cost estimate should not be overly conservative or optimistic, and should be, among other things, based on an assessment of most likely costs, adjusted properly for inflation, and validated against an independent cost estimate. In addition, the estimate should be updated regularly to reflect material changes in the program and actual cost experience on the program. Further, steps should be taken to minimize mathematical mistakes and their significance and to ground the estimate in documented assumptions and a historical record of actual cost and schedule experiences on comparable programs.

- *Credible:* The cost estimate should discuss any limitations in the analysis due to uncertainty or biases surrounding the data and assumptions. Major assumptions should be varied and other outcomes computed to determine how sensitive the estimate is to changes in the assumptions. Risk and uncertainty inherent in the estimate should be assessed and disclosed. Further, the estimate should be properly verified by, for example, comparing the results with one or more independent cost estimates.

  The SPO's Block 1 life cycle cost estimate includes the costs to complete those portions of Block 1 that are to be deployed to the Tucson and Yuma Sectors, which together cover about 387 miles of the southwest border (53 miles associated with both TUS-1 and AJO-1, which are in the Tucson Sector, as well as an additional 209 miles in the Tucson Sector and 125 miles in the Yuma Sector). More specifically, this estimate, which is dated December 2008, shows the minimum cost to acquire and deploy Block 1 to the Tucson and Yuma Sectors to be $758 million, with another $544 million to operate and maintain this initial capability, for a total of about $1.3 billion.

  However, this Block 1 cost estimate is not reliable because it does not sufficiently possess any of the above four characteristics. Specifically:

- The estimate is not comprehensive because it does not include all relevant costs, such as support contractor costs and costs associated with system and software design, development, and testing activities that were incurred prior to December 2008. Moreover, it includes only 1 year of operations and maintenance costs rather than these costs over the expected life of the system. Further, the estimate does not document and assess the risks associated with all ground rules and assumptions, such as known budget constraints, staff and schedule variations, and technology maturity.

- The estimate is not well-documented because, among other things, the sources and significance of key data have not been captured and the quality of key data, such as historical costs and actual cost reports, is limited. For example, instead of identifying and relying on historical costs from similar programs, the estimate was based, in part, on engineering judgment. Further, the calculations performed and their results, while largely documented, did not document contingency reserves and the associated confidence level for the risk-adjusted cost estimate. Also, as noted above, assumptions integral to the estimate, such as those for budget constraints, and staff and schedule variances, were not documented.

- The estimate is not accurate because it was not, for example, validated against an independent cost estimate. Further, it has not been updated to reflect material program changes since the estimate was developed. For example, the estimate does not reflect development and testing activities that were added since the estimate was approved to correct problems discovered during testing. Further, the estimate has not been updated with actual cost data available from the contractor.

- The estimate is not credible because its inherent risk and uncertainty were not adequately assessed, and thus the estimate does not address limitations associated with the assumptions used to create it. For example, the risks associated with software development were not examined, even though such risks were known to exist. In fact, the only risks considered were those associated with uncertainty in labor rates and hardware costs, and instead of being based on historical quantitative analyses, these risks were expressed by assigning them arbitrary positive or negative percentages. In addition, and for the reasons mentioned above, the estimate did not specify contingency reserve amounts to mitigate known risks, and an independent cost estimate was not used to verify the estimate.

Program officials attributed these limitations in the cost estimate's comprehensiveness, documentation, accuracy, and credibility to a range of factors, including competing program office priorities and the department's limited cost estimating capabilities. For example, program officials stated that the DHS Cost Analysis Division did not prepare an independent estimate because it did not have, among other things, the people and tools needed to do so. In this regard, this division reports that as of July 2009, DHS only had eight cost estimators (six in headquarters and two in program offices) for departmentwide needs.

Because the estimate does not adequately display these four characteristics, it does not provide a reliable picture of Block 1's life cycle costs. As a result, DHS does not have complete information on which to base informed investment decision making, understand system affordability, and develop justifiable budget requests. Moreover, the Block 1 cost estimate does not provide a meaningful standard against which to measure cost performance, is likely to show large cost overruns, and does not provide a good basis for informing future cost estimates.

Expected Mission Benefits Have Yet to Be Adequately Defined

The Clinger-Cohen Act of 1996 and OMB guidance[34] emphasize the need to ensure that IT investments actually produce tangible, observable improvements in mission performance. As we have previously reported,[35] to accomplish this, benefits that are expected to accrue from investments need to be forecast and their actual accrual needs to be measured.

In the case of Block 1, however, expected mission benefits have not been defined and measured. For example, while program officials told us that system benefits are documented in the SBI*net* Mission Need Statement dated October 2006, this document does not include either quantifiable or qualitative benefits. Rather, it provides general statements such as "the lack of a program such as SBI*net* increases the risks of terrorist threats and other illegal activities."

[34]Clinger-Cohen Act of 1996, 40 U.S.C. sections 11101-11704, and OMB, Circular No. A-130, *Management of Federal Information Resources* (Washington, D.C., Nov. 30, 2000).

[35]GAO, *DOD Business Systems Modernization: Planned Investment In Navy Program to Create Cashless Shipboard Environment Needs to be Justified and Better Managed*, GAO-08-922 (Washington, D.C.: Sept. 8, 2008).

Congress recognized the importance of having a meaningful understanding of SBI*net*'s value proposition when it required DHS in 2008 to provide in its Border Security, Fencing, Infrastructure, and Technology Fiscal Year 2009 Expenditure Plan[36] a description of how the department's planned expenditure of funds would be linked to expected SBI mission benefits and outcomes. However, we reported that the plan DHS submitted only described links among planned activities, expenditures, and outputs. It did not link these to outcomes associated with improving operational control of the border.[37] More recently, we reported that while SBI technology and physical infrastructure, along with increases in Border Patrol personnel, are intended to allow DHS to gain effective control of U.S. borders, CBP's measures of effective control are limited. Thus, we recommended that CBP conduct a cost-effectiveness evaluation of the SBI tactical infrastructure's impact on effective control of the border, and DHS agreed with this recommendation.[38] Further, program officials noted that uncertainty about SBI*net*'s role in and contribution to effective control of the border makes it difficult to forecast SBI*net* benefits. Rather, they said that operational experience with Block 1 is first needed in order to estimate such benefits.

While we recognize the value of operationally evaluating an early, prototypical version of a system in order to better understand, among other things, its mission impact, and thus to better inform investment decisions, we question the basis for spending in excess of a billion dollars to gain this operational experience. Without a meaningful understanding and disclosure of SBI*net* benefits, to include the extent to which expected mission benefits are known and unknown, DHS did not have the necessary basis for justifying and making informed decisions about its sizeable investment in Block 1, as well as for measuring the extent to which the deployed Block 1 will actually deliver mission value commensurate with costs.

[36]Pub. L. No. 110-329, 122 Stat. 3574, 3655-57 (2008).

[37]GAO, *U.S. Customs and Border Protection's Secure Border Initiative Fiscal Year 2009 Expenditure Plan*, GAO-09-274R (Washington, D.C.: Apr. 30, 2009).

[38]GAO-09-896.

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

Successful management of large IT programs, like SBI*net*, depends in large part on having clearly defined and consistently applied life cycle management processes. Our evaluations and research show that applying system life cycle management rigor and discipline increases the likelihood of delivering expected capabilities on time and within budget.[39] In other words, the quality of a system is greatly influenced by the quality of the processes used to manage it.

To the SPO's credit, it has defined key life cycle management processes that are largely consistent with relevant guidance and associated best practices. However, it has not effectively implemented these processes. Specifically, it has not consistently followed its systems engineering plan, requirements development and management plan, and risk management approach. Reasons cited by program officials for not implementing these processes include the decision by program officials to rely on contract task order requirements that were developed prior to the systems engineering plan, and competing SPO priorities, including meeting an aggressive deployment schedule. Until the SPO consistently implements these processes, it will remain challenged in its ability to successfully deliver SBI*net*.

Key System Life Cycle Management Activities Have Not Been Consistently Performed

Each of the steps in a life cycle management approach serves an important purpose and has inherent dependencies with one or more other steps. In addition, the steps used in the approach should be clearly defined and repeatable. Thus, if a life cycle management step is omitted or not performed effectively, later steps can be affected, potentially resulting in costly and time-consuming rework. For example, a system can be effectively tested to determine whether it meets requirements only if these requirements have been completely and correctly defined. To the extent that interdependent life cycle management steps or activities are not effectively performed, or are performed concurrently, a program will be at increased risk of cost, schedule, and performance shortfalls.

The SPO's Systems Engineering Plan documents its life cycle management approach for SBI*net* definition, development, testing, deployment, and sustainment. As noted earlier, we reported in September 2008 on a number

[39]See, for example, GAO, *Homeland Security: Despite Progress, DHS Continues to Be Challenged in Managing Its Multi-Billion Dollar Investment in Large-Scale Information Technology Systems*, GAO-09-1002T (Washington, D.C.: Sept. 15, 2009) and GAO-08-1086.

of weaknesses in the SBI*net* life cycle management approach and made recommendations to improve it.[40] In response, the SPO revised its Systems Engineering Plan in November 2008, and to its credit, the revised plan is largely consistent with DHS and other relevant guidance.[41] For example, it defines a number of key life cycle milestone or "gate" reviews that are important in managing the program, such as initial planning reviews, requirements reviews, system design reviews, and test reviews. In addition, the revised plan requires most of the key artifacts and program documents that DHS guidance identified as important to each gate review, such as a concept of operations, an operational requirements document, a deployment plan, a risk management plan, a life cycle cost estimate, requirements documentation, and test plans. To illustrate, the plan identifies CDR as the important milestone event where a design baseline is to be established, requirements traceability is to be demonstrated, and verification and testing plans are to be in place.

However, the Systems Engineering Plan does not address the content of the key artifacts that it requires. For example, it does not provide a sample document or content template for the concept of operations, the operational requirements document, or the deployment plan. As a result, the likelihood of the developers and reviewers of these artifacts sharing and applying a consistent and repeatable understanding of their content is minimized, thus increasing the risk that they will require costly and time-consuming rework. As we recently reported,[42] the absence of content guidance or criteria for assessing the quality of the prime contractor's test-related deliverables was a primary reason that limitations were found in test plans.

Beyond the content of the Systems Engineering Plan, the SPO has not consistently implemented key system life cycle management activities for Block 1 that are identified by the plan. For example, the following artifacts were not reviewed or considered during the CDR that concluded in October 2008:

[40]GAO-08-1086.

[41]Department of Homeland Security, *Acquisition Instruction/Guidebook*, *102-01-001*, *Appendix B*, *Systems Engineering Life Cycle*, Interim Version 1.9 (Nov. 7, 2008); and *IEEE Standard for Application and Management of the Systems Engineering Process*, IEEE Std. 1220-2005 (New York, N.Y., Sept. 9, 2005).

[42]GAO-10-158.

- Security Test Plan, which describes the process for assessing the robustness of the system's security capabilities (e.g., physical facilities, hardware, software, and communications) in light of their vulnerabilities.

- Quality Plan, which documents the process for verifying that the contractor deliverables satisfy contractual requirements and meet or exceed quality standards.

- Test Plan, which describes the overall process for the test and evaluation, including the development of detailed test event plans, test procedure instructions, data collection methods, and evaluation reports.

- Block Training Plan, which outlines the objectives, strategy, and curriculum for training that are specific to each block, including the activities needed to support the development of training materials, coordination of training schedules, and reservation of personnel and facilities.

- Block Maintenance Plan, which lays out the policies and concepts to be used to maintain the operational availability of hardware and software.

To the SPO's credit, it reviewed and considered all but one of the key artifacts for the TUS-1 Deployment Readiness Review that concluded in April 2009. The omitted artifact was the Site Specific Training Plan, which outlines the objectives, strategy, and curriculum for training that are specific to each geographic site, including the activities needed to support the development of training materials, coordination of training schedules, and reservation of personnel and facilities. According to program officials, even though the Systems Engineering Plan cites the training plan as integral to the Deployment Readiness Review, this training plan is to be reviewed as part of a later milestone review.

Program officials stated that a reason that the artifacts were omitted is that they have yet to begin implementing the Systems Engineering Plan. Instead, they have, for example, enforced the CDR requirements in the System Task Order that Boeing was contractually required to follow. To address this, they added that the SPO intends to bring the task orders into alignment with the Systems Engineering Plan, but they did not specify when this would occur. As a result, key milestone reviews and decisions have not always benefited from life cycle management documentation that the SPO has determined to be relevant and important to these milestone events. More specifically, the Systems Engineering Plan states that the gate reviews are intended to identify and address problems early and thus

minimize future costs and avoid subsequent operational issues. By not fully informing these gate reviews and associated decisions with key life cycle management documentation, the risk of Block 1 design and deployment problems is increased, as is the likelihood of expensive and time-consuming system rework.

Key Block 1 Requirements Have Not Been Adequately Developed and Managed

Well-defined and managed requirements are essential to successfully acquiring large-scale systems, like SBI*net*. According to relevant guidance,[43] effective requirements development and management include establishing a baseline set of requirements that are complete, unambiguous, and testable. It also includes ensuring that system-level requirements are traceable backwards to higher-level operational requirements and forward to design requirements and the methods used to verify that they are met. Among other things, this guidance states that such traceability should be used to verify that higher-level requirements have been met by first verifying that the corresponding lower-level requirements have been satisfied.

However, not all Block 1 component requirements were sufficiently defined at the time that they were baselined, and operational requirements continue to be unclear and unverifiable. In addition, while requirements are now largely traceable backwards to operational requirements and forward to design requirements and verification methods, this traceability has not been used until recently to verify that higher-level requirements have been satisfied. Program officials attributed these limitations to competing SPO priorities, including aggressive schedule demands. Without ensuring that requirements are adequately defined and managed, the risks of Block 1 not performing as intended, not meeting user needs, and costing more and taking longer than necessary to complete are increased.

Not All Requirements Were Adequately Baselined

The SBI*net* Requirements Development and Management Plan states that a baseline set of requirements should be established by the time of the CDR and that these requirements should be complete, unambiguous, and testable. Further, the program's Systems Engineering Plan states that the CDR is intended to establish the final allocated requirements baseline and ensure that system development, integration, and testing can begin.

[43]Software Engineering Institute (SEI), Capability Maturity Model Integration (CMMI)® for Acquisition, Version 1.2 (Pittsburgh, Penn., November 2007).

To the SPO's credit, it established a baseline set of requirements for the TUS-1 and AJO-1 system deployments at CDR. However, the baseline requirements associated with the NOC/SOC were not adequately defined at this time, as evidenced by the fact that they were significantly changed 2 months later. Specifically, about 33 percent of the component-level requirements and 43 percent of the design specifications for NOC/SOC were eliminated from the Block 1 design after CDR. Program officials attributed these changes to the NOC/SOC requirements to (1) requirements that were duplicative of another specification, and thus were redundant; (2) requirements that were poorly written, and thus did not accurately describe needs; and (3) requirements that related to the security of a system that SBI*net* would not interface with, and thus were unnecessary.

According to program officials, the NOC/SOC was a late addition to the program, and at the time of CDR, the component's requirements were known to need additional work. Further, they stated that while the requirements were not adequately baselined at the time of CDR, the interface requirements were understood well enough to begin system development.

Without properly baselined requirements, system testing challenges are likely to occur, and the risk of system performance shortfalls, and thus cost and schedule problems, are increased. In this regard, we recently reported that NOC/SOC testing was hampered by incorrect mapping of requirements to test cases, failure to test all of the requirements, and significant changes to test cases made during the testing events.[44] This occurred in part because ambiguities in requirements caused testers to rewrite test steps during execution based on interpretations of what they thought the requirements meant, and they required the SPO to conduct multiple events to test NOC/SOC requirements.

Block 1 Operational Requirements Remain Poorly Defined

According to the SBI*net* Requirements Development and Management Plan, requirements should be achievable, verifiable, unambiguous, and complete. To ensure this, the plan contains a checklist that is to be used in verifying that each requirement possesses these characteristics.

However, not all of the SBI*net* operational requirements that pertain to Block 1 possess these characteristics. Specifically, a November 2007 DHS

[44] GAO-10-158.

assessment[45] determined that 19 operational requirements, which form the basis for the lower-level requirements used to design and build the system, were not complete, achievable, verifiable, or affordable. Further, our analysis of the 12 Block 1 requirements that are included in these 19 operational requirements shows that they have not been changed to respond to the DHS findings.[46] According to the assessment, 6 of the 12 were unaffordable and unverifiable, and the other 6 were incomplete. Examples of these requirements and DHS's assessment follow:

- A requirement that the system should provide for complete coverage of the border was determined to be unverifiable and unaffordable because defining what complete coverage meant was too difficult and ensuring complete coverage, given the varied and difficult terrain along the border, was cost prohibitive.

- A requirement that the system should be able to detect and identify multiple simultaneous events with different individuals or groups was determined to be incomplete because the requirement did not specify the number of events to be included, the scope of the area to be covered, and the system components to be involved.

As we have previously reported,[47] these limitations in the operational requirements affect the quality of system, component, and software requirements. This is significant because, as of September 2009, these 12 operational requirements were associated with 16 system-level requirements, which were associated with 152 component-level requirements, or approximately 15 percent of the total number of component-level requirements. According to program officials, these requirements were not updated because the SPO planned to resolve the problems through the testing process. However, we recently reported that requirements limitations actually contributed to testing challenges.[48] Specifically, we reported that about 71 percent of combined system

[45]SBI*net* Program Deep Dive Review (Nov. 26, 2007).

[46]Of the12 requirements, 11 were unchanged, and while the remaining requirement was slightly modified, nothing was added to this requirement to address the DHS findings.

[47]GAO-08-1086.

[48]GAO-10-158.

qualification and component qualification[49] test cases had to be rewritten extemporaneously during test execution. According to program officials, this was partly due to ambiguities in requirements, which led to differing opinions among the program and contractor staff about what was required to effectively demonstrate that the requirements were met.

Further, program officials stated that a number of requirements have been granted deviations or waivers because they were poorly written. For example:

- A requirement for camera equipment to "conform to the capabilities and limitations of the users to operate and maintain it in its operational environment and not exceed user capabilities" was determined to be subjective and unquantifiable and thus was waived.
- A requirement for the tower design to accommodate the future integration of components "without causing impact on cost, schedule, and/or technical performance" was determined to have no specific criteria to objectively demonstrate closure decision and thus was also waived.

As a result of these deviations and waivers, the system capabilities that are to be delivered as part of Block 1 will be less than originally envisioned.

Requirements Traceability Has Improved, but Until Recently Has Not Been Used To Determine If Operational Requirements Were Met

Consistent with relevant guidance,[50] the SBI*net* Requirements Development and Management Plan provides for maintaining bidirectional traceability from high-level operational requirements through detailed low-level requirements to test plans. More specifically, it states that operational requirements should trace to system requirements, which in turn should trace to component requirements that trace to design requirements, which further trace to verification methods.

Since September 2008, the SPO has worked with Boeing to manually review each requirement and develop a bidirectional traceability matrix. Further, it has used this matrix to update the DOORS requirements database. Our analysis of the traceability of a random sample of Block 1 component-level requirements in the DOORS database shows that they are

[49]System qualification testing verifies that the system design satisfies system-level requirements, and component qualification testing verifies that components satisfy performance requirements.

[50]SEI, CMMI® for Acquisition.

largely traceable backwards to operational requirements and forward to design requirements and verification methods. For example, we estimate that only 5 percent (with a 95 percent confidence interval between 1 and 14 percent) of a random sample of component requirements cannot be traced to the system requirements and then to the operational requirements. In addition, we estimate that 0 percent (with a 95 percent confidence interval between 0 and 5 percent) of the component requirements in the same sample do not trace to a verification method. (See table 5 for the results of our analysis along with the associated confidence intervals.) [51]

Table 5: SBI*net* Requirements Traceability Results

Traceability links from component requirements	Estimated failure rate	95 percent confidence interval
To system requirement then to operational requirement	5%	1-14%
To system requirement	3	0-11
To verification method	0	0-5

Source: GAO analysis of DHS data.

By establishing this traceability, the SPO is better positioned to know the extent to which the acquired and deployed system can meet operational requirements.

However, the SPO has not used its requirements traceability in closing higher-level component requirements. According to relevant guidance, [52] all lower-level requirements (i.e., children) should be closed in order to sufficiently demonstrate that the higher-level requirements (i.e., parents) have been met. Consistent with this guidance, the SBI*net* Requirements Development and Management Plan states that ensuring the traceability of requirements from children to their parents is an integral part of ensuring that testing is properly planned and conducted. However, 4 of 8 higher-level component requirements (parents) in the above cited random sample of system-level requirements were closed regardless of whether their corresponding lower-level design requirements (children) had been

[51] An insufficient number of design requirements were sampled to generalize the results for the entire database. However, all design requirements that we sampled traced to a verification method.

[52] SEI, CMMI® for Acquisition.

closed. According to program officials, this is because their standard practice in closing parent requirements, until recently, was to sometimes close them before their children were closed. Further, they said that this was consistent with their verification criteria[53] for closing higher-level requirements, which did not require closure of the corresponding lower-level requirements. They also said that the reason parent verification criteria did not always reflect children verification criteria was that traceability was still being established when the verification criteria were developed and thus parent-child relationships were not always available to inform the closure criteria. Furthermore, they stated that schedule demands did not permit them to ensure that the verification criteria for requirements were aligned with the traceability information.

After we shared our findings on parent requirement closure with the SPO, officials stated that they had changed their approach and will no longer close parent requirements without ensuring that all of the children requirements have first been closed. However, they did not commit to reviewing previously closed parents to determine that all of the children were closed. Without fully ensuring traceability among requirements verification methods, the risks of delivering a system solution that does not fully meet user needs or perform as intended, and thus requires additional time and resources to deliver, are increased.

Key Risks Have Not Been Effectively Managed and Disclosed

Risk management is a continuous, forward-looking process that effectively anticipates and mitigates risks that may have a critical impact on a program's success. In 2008, the SPO documented a risk management approach[54] that largely complies with relevant guidance. However, it has not effectively implemented this approach for all risks. Moreover, available documentation does not demonstrate that significant risks were disclosed to DHS and congressional decision makers in a timely fashion, as we previously recommended and, while risk disclosure to DHS leadership has recently improved, not all risks have been formally captured and thus shared. As a result, the program will likely continue to

[53]Verification criteria are assigned to each requirement and, according to program officials, are used to determine that a requirement has been satisfied, and therefore can be considered "closed."

[54]This approach is described in three documents: the SBI*net* Risk Management Plan, dated June 6, 2008; the SBI*net* SPO Risk/Issue/Opportunity Management Process, dated October 9, 2008; and the SBI*net* Risk Management Policy, dated November 6, 2008.

experience actual cost, schedule, and performance shortfalls, and key decision makers will continue to be less than fully informed.

Risk Management Approach Has Been Adequately Defined

According to relevant guidance,[55] effective risk management includes defining a process that, among other things, proactively identifies and analyzes risks on the basis of likelihood of occurrence and impact, assigns ownership, provides for mitigation, and monitors status. To the SPO's credit, it has developed an approach for risk management that is largely consistent with this guidance. For example, the approach provides for

- continuously identifying risks throughout the program's life cycle before they develop into actual problems, including suggested methods for doing so, such as conducting brainstorming sessions and interviewing subject matter experts;
- analyzing identified risks to determine their likelihood of occurring and potential impact;
- assigning responsibility for risks;
- developing a risk mitigation plan, to include a set of discrete, measurable actions or events which, if successfully accomplished, can avoid or reduce the likelihood of occurrence or severity of impact of the risk; and
- executing and regularly monitoring risk mitigation plans to ensure that they are implemented and to allow for corrective actions if the desired results are not being achieved.

In February 2007, we reported that the program's risk management approach was in the process of being established.[56] Specifically, we noted that at that time the SPO had drafted a risk management plan, established a governance structure, developed a risk management database, and identified 30 risks. In April 2009, we reported that the DHS Chief Information Officer had certified that this approach provided for the regular identification, evaluation, mitigation, and monitoring of risks

[55]SEI, CMMI® for Acquisition.

[56]GAO-07-309.

throughout the system life cycle, and that it provided for communicating high-risk conditions to DHS investment decision makers.[57]

Risk Management Approach Has Not Been Fully Implemented, although Improvements Are Under Way

The SPO has not adhered to key aspects of its defined process for managing program risks. In particular, the program's risk management repository, which is the tool used for capturing and tracking risks and their mitigation, has not included key risks that have been identified by stakeholders. For example, our analysis of reports from the repository showing all open and closed risks from April 2006 to September 2009 shows that the following program risks that have been identified by us and others were not captured in the repository:

- program cost and schedule risks briefed by the SPO to senior SBI*net* officials in January 2009, such as unplanned and unauthorized work impacting the credibility of the program cost data, and program costs and schedule plans lacking traceability;
- program schedule and cost estimate risks identified by the Defense Contract Management Agency prior to March 2009, such as contractor-provided documentation not permitting adequate assessment of critical path accuracy, and cost projections not including all applicable elements and thus lacking credibility; and
- the risk of the SPO's heavy reliance on contractors, reported by the DHS Office of Inspector General in June 2009.

In addition, the SBI Executive Director told us that the program faces a number of other risks, all but one of which were also not in the repository. These include the lack of well-defined acquisition management processes, staff with the appropriate acquisition expertise, and agreement on key system performance parameters. According to program officials, some of these risks are not in the repository because Boeing is responsible for operating and maintaining the repository, and the specifics surrounding the risks and their mitigation are considered acquisition sensitive, meaning that they should not be shared with Boeing. In this regard, the officials acknowledged that the SPO needs a risk database independent of the contractor to manage these acquisition-sensitive risks.

[57] GAO-09-274R.

Further, the Risk Manager identified other limitations that have hindered the SPO's risk management efforts, along with recent actions intended to address them. For example:

- Risk review meetings were only being held once a month, which was resulting in lost opportunities to mitigate risks that were to be realized as actual problems within 30 days. As a result, the frequency of these meetings has been increased to twice a month.

- Risk information provided to senior SBI managers at monthly Joint Program Management Review Meetings[58] was not sufficiently detailed, and thus has been expanded.

- Changes were being made to the risk management repository by contractor staff without sufficient justification and without the approval of the Joint Risk Review Board. For example, program officials cited an instance in which a risk's severity was changed from medium to high and no board member knew the reason for the change. As a result, the number of contractor staff authorized to modify data in the repository was reduced.

- The repository did not include all requisite information for all identified risks. For example, some risks were missing the rationale for the likelihood of occurrence and the potential impact. As a result, the Joint Risk Review Board has adopted a policy of not accepting risks that are missing requisite information.

According to the Risk Manager, competing program priorities have resulted in insufficient resources devoted to risk management activities, which has contributed to the state of the SPO's risk management efforts. However, he added that the SPO is taking steps to improve risk management by revising risk management guidance, implementing a CBP-approved database tool for managing government-only risks, and increasing risk management training and oversight.

Until the program's risk management is strengthened and effectively implemented, the program will continue to be challenged in its ability to forestall cost, schedule, and performance problems.

[58]The Joint Program Management Review meetings take place on a monthly basis to discuss program status. They are attended by program officials, contractor senior staff, and such key stakeholders as Border Patrol, Air and Marine, Office of Intelligence, Office of Information Technology, and Office of Asset Management.

Risks Have Not Been Fully Disclosed, but Improvement Has Recently Occurred

As noted earlier, we recommended in September 2008 that the SPO assess SBI*net* risks and that the results of these assessments, along with alternative courses of action to address them, be provided to DHS leadership and congressional committees.[59] According to program officials, shortly after receiving our draft report they briefed the DHS Acquisition Review Board[60] on, among other things, SBI*net* risks. However, the briefing slides used for this meeting do not identify individual risks. Instead, the briefing contains one slide that only identifies "contributing factors" to changes in the program's schedule, including a reallocation SBI*net* funding to SBI physical infrastructure, concurrencies and delays that have occurred in testing, and the need for environmental studies. The slides do not identify risks and alternative courses of action to address or mitigate them.

In addition, program officials told us that they briefed congressional committees during the fall of 2008 on the program's status, which they said included disclosure of program risks. However, they did not have any documentation of these briefings to show which committees were briefed, when the briefings occurred, who was present, and what was discussed and disclosed. Further, House Committee on Homeland Security staff stated that while program officials briefed them following our September 2008 report, specific program risks were not disclosed. As a result, it does not appear that either DHS or congressional stakeholders received timely information on risks facing the program at a crucial juncture in its life cycle.

To the SPO's credit, it has recently improved its disclosure of risks facing the program. In particular, the SBI Executive Director briefed the DHS Chief Information Officer in November 2009 on specific program risks. However, this briefing states that the risks presented were the Block 1 risks as captured in the contractor's risk repository and that additional risks have not yet been formalized (see above discussion about repository limitations). Until all key risks are formally managed and regularly disclosed to department and congressional stakeholders, informed SBI*net* investment decision making will be constrained.

[59]GAO-08-1086.

[60]This board is chaired by the Deputy Secretary and includes a number of senior DHS leaders.

DHS Has Yet to Implement GAO's Recent SBI*net* Recommendations

As noted earlier, we reported on a number of SBI*net* program management weaknesses in September 2008, and we concluded that these weaknesses introduced considerable risk that the program would not meet expectations and would require time-consuming and expensive rework.[61] In summary, these problems included a lack of clarity and certainty surrounding what technological capabilities would be delivered when, and a lack of rigor and discipline around requirements definition and management and test management. To address these problems and thereby reduce the program's exposure to cost, schedule, and performance risks, we made eight recommendations. DHS concurred with seven of the recommendations and disagreed with one aspect of the remaining one.

In summary, the department has not implemented two of the recommendations and has partially implemented the remaining six. See table 6 for a summary and appendix III for a detailed discussion of the status of each recommendation.

Table 6: Summary of DHS Implementation of GAO's Recent SBI*net* Recommendations

Recommendation	DHS comment	Status
(1/2) Assess risks associated with the SBI*net* acquisition and provide the results of the risk assessment to DHS senior leadership and congressional authorization and appropriation committees	Concurred	Not implemented
(3) Establish and baseline the program commitments	Concurred	Partially implemented
(4) Finalize and approve an integrated master schedule	Concurred	Partially implemented
(5) Revise and approve consistent and up-to-date versions of the SBI*net* life cycle management approach that reflect relevant federal guidance and leading practices	Concurred	Partially implemented
(6) Implement the revised life cycle management approach	Concurred	Partially implemented
(7) Implement key practices for developing and managing system requirements	Concurred	Partially implemented
(8) Implement key test management practices	Partially disagreed	Partially implemented

Source: GAO analysis of DHS data.

Note: "Partially implemented" means that some, but not all, aspects of the recommendation have been fully implemented. "Not implemented" means that none of the aspects of the recommendation have been fully implemented.

[61] GAO-08-1086.

Conclusions

DHS has yet to demonstrate that its proposed SBI*net* solution is a cost-effective course of action, and thus whether the considerable time and money being invested to acquire and deploy it is a wise and prudent use of limited resources. Given that the magnitude of the initial investment in SBI*net* spans more than 3 years of effort and totals hundreds of millions of dollars, coupled with the fact that the scope of the initial system's capabilities and areas of deployment have continued to shrink, the program is fraught with risk and uncertainty. As a result, the time is now for DHS to thoughtfully reconsider its proposed SBI*net* solution, and in doing so, to explore ways to both limit its near-term investment in an initial set of operational capabilities and develop and share with congressional decision makers reliable projections of the relative costs and benefits of longer-term alternatives for meeting the mission goals and outcomes that SBI*net* is intended to advance, or reasons why such information is not available and the uncertainty and risks associated with not having it.

Compounding the risks and uncertainty surrounding whether the department is pursuing the right course of action are a number of system life cycle management concerns, including limitations in the integrated master schedule; shortcomings in the documentation available to inform key milestone decisions; and weaknesses in how requirements have been developed and managed, risks have been managed, and tests have been conducted. Collectively, these concerns mean that the program is not employing the kind of acquisition management rigor and discipline needed to reasonably ensure that proposed system capabilities and benefits will be delivered on time and on budget.

Because of SBI*net*'s decreased scope, uncertain timing, unclear costs relative to benefits, and limited life cycle management discipline and rigor, in combination with its size and mission importance, the program represents a risky undertaking. To minimize the program's exposure to risk, it is imperative for DHS to move swiftly to first ensure that SBI*net*, as proposed, is the right course of action for meeting its stated border security and immigration management goals and outcomes, and once this is established, for it to move with equal diligence to ensure that it is being managed the right way. To this end, our prior recommendations to DHS relative to SBI*net* provide for strengthening a number of life cycle management processes, including requirements development and management and test management. Accordingly, we are not making additional recommendations that focus on these processes at this time.

Recommendations for Executive Action

To address the considerable risks and uncertainties facing DHS on its SBI*net* program, we are making 12 recommendations. Specifically, we recommend that the Secretary of Homeland Security direct the Commissioner of U.S. Customs and Border Protection to limit future investment in the program to only work that meets one or both of the following two conditions: (1) is already under contract and supports deployment, acceptance, and operational evaluation of only those Block 1 capabilities (functions and performance levels) that are currently targeted for TUS-1 and AJO-1; or (2) provides the analytical basis for informing a departmental decision as to what, if any, expanded investment in SBI*net*, both in terms of capabilities (functions and performance) and deployment locations, represents a prudent, responsible, and affordable use of resources for achieving the department's border security and immigration management mission.

With respect to the first condition, we further recommend that the Secretary of Homeland Security direct the Commissioner of U.S. Customs and Border Protection to have the SBI Executive Director make it a program priority to ensure that

- the integrated master schedule for delivering Block 1 capabilities to TUS-1 and AJO-1 is revised to address the key schedule estimating practices discussed in this report;
- the currently defined Block 1 requirements, including key performance parameters, are independently validated as complete, verifiable, and affordable and any limitations found in the requirements are addressed;
- the Systems Engineering Plan is revised to include or reference documentation templates for key artifacts required at milestone gate reviews;
- all parent requirements that have been closed are supported by evidence of the closure of all corresponding and associated child requirements; and
- all significant risks facing the program are captured, mitigated, tracked, and periodically reported to DHS and congressional decision makers.

Also with respect to the first condition, we reiterate our prior recommendations, as stated in our September 2008 report,[62] relative to

[62]GAO-08-1086.

establishing program commitments, implementing the Systems Engineering Plan, defining and managing requirements, and testing.

With respect to the second condition, we further recommend that the Secretary of Homeland Security direct the Commissioner of U.S. Customs and Border Protection to have the SBI Executive Director make it a program priority to ensure that

- a life cycle cost estimate for any incremental block of SBI*net* capabilities that is to include capabilities and cover locations beyond those associated with the TUS-1 and AJO-1 deployments is developed in a manner that reflects the four characteristics of a reliable estimate discussed in this report;
- a forecast of the qualitative and quantitative benefits to be derived from any such incremental block of SBI*net* over its useful life, or reasons why such forecasts are not currently possible, are developed and documented;
- the estimated life cycle costs and benefits and associated net present value of any such incremental block of SBI*net* capabilities, or reasons why such an economic analysis cannot be performed, are prepared and documented; and
- the results of these analyses, or the documented reasons why such analyses cannot be provided, are provided to the Commissioner of U.S. Customs and Border Protection and the DHS Acquisition Review Board.

Also with respect to this second condition, we recommend that the Secretary of Homeland Security direct the Deputy Secretary of Homeland Security, as the Chair of the DHS Acquisition Review Board, to (1) decide, in consultation with the board and Commissioner of U.S. Customs and Border Protection, what, if any, expanded investment in SBI*net*, both in terms of capabilities (functions and performance) and deployment locations, represents a prudent, responsible, and affordable use of resources for achieving the department's border security and immigration management mission; and (2) report the decision, and the basis for it, to the department's authorization and appropriations committees.

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, DHS stated that it agreed with ten of our recommendations and partially agreed with the remaining two. In this regard, it described

ongoing and planned actions to address each, and it provided milestones for completing these actions. In addition, DHS provided technical comments, which we have incorporated in the report as appropriate.

In agreeing with our first recommendation, however, DHS commented that the words "one of" were omitted before the two conditions contained in the recommendation. However, this interpretation is not correct. Rather, the intent of our recommendation is to limit future investment on the program to either of the conditions, meaning "one or both of." Notwithstanding DHS's interpretation, we believe that actions that it described to address this recommendation, which include freezing funding beyond the initial deployments to TUS-1 and AJO-1 until it completes a comprehensive reassessment of the program that includes an analysis of the cost and mission effectiveness of alternative technologies, is consistent with the intent of the recommendation. Nevertheless, we have slightly modified the recommendation to avoid any further confusion.

Regarding its partial agreement with our recommendation for revising the integrated master schedule in accordance with a range of best practices embodied in our cost and schedule estimating guide, DHS acknowledged the merits of employing these practices and stated that it is committed to adopting and deploying them. However, it added that the current contract structure limits its ability to fully implement all the practices prior to completing the TUS-1 and AJO-1 deployments. We understand that program facts and circumstances create practical limitations associated with some of the practices, and believe that DHS's planned actions are consistent with the intent of our recommendation.

Regarding its partial agreement with our recommendation that reiterated a number of the recommendations that we made in a prior report,[63] DHS stated that, while these prior recommendations reflect program management best practices and it continues to make incremental improvements to address each, the scope of the program had narrowed since these recommendations were made. As a result, DHS stated that these prior recommendations were not fully applicable until and unless a decision was made to move the program forward and conduct future deployments beyond TUS-1 and AJO-1. We acknowledge that the facts and circumstances surrounding the program have recently changed and that these changes impact the nature and timing of actions appropriate for

[63]GAO-08-1086.

implementing them. Moreover, we believe that DHS's planned actions are consistent with the intent of our recommendation.

DHS also commented that it believed that it had implemented two of our recommendations and that these recommendations should be closed. Because closure of our recommendations requires evidentiary validation of described actions, and because many of the actions that DHS described were planned rather than completed, we are not closing any of our recommendations at this time. As part of our recurring review of the status of all of our open recommendations, we will determine if and when the recommendations have been satisfied and thus can be closed.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to interested congressional committees and other parties. We will also send copies to the Secretary of Homeland Security, the Commissioner of the 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 you or 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 Offices 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 VI.

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

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine the extent to which the Department of Homeland Security (DHS) has (1) defined the scope of its proposed Secure Border Initiative Network (SBI*net*) solution, (2) developed a reliable schedule for delivering this solution, (3) demonstrated the cost-effectiveness of this solution, (4) acquired this solution in accordance with key life cycle management processes, and (5) addressed our recent SBI*net* recommendations. To accomplish our objectives, we largely focused on the first increment of SBI*net*, known as Block 1.

To determine the extent to which DHS has defined the scope of its proposed system solution, we reviewed key program documentation related to the Block 1 functional and performance requirements and deployment locations, such as the SBI*net* Acquisition Program Baseline and related acquisition decision memorandums, the Operational Requirements Document, the Operational Requirements Document Elements Applicable to Block 1 System, the Requirements Traceability Matrix, the Requirements Verification Matrix, and the SBI*net* Block 1 User Assessment. In addition, we compared Block 1 requirements that were baselined in October 2008 as part of the Critical Design Review (CDR) to the Block 1 requirements as defined as of September 2009 to identify what, if any, changes had occurred, and we interviewed program officials as to the reasons for any changes. We also compared the locations, including the miles of border associated with these locations, that were to receive Block 1 as of September 2008 to the locations specified in the program's March 2009 Acquisition Program Baseline to identify any changes, and we interviewed program officials as to the reasons for any changes. Further, we compared the key performance parameters listed in the Operational Requirements Document, dated March 2007, to the key performance parameters in the program's Acquisition Program Baseline dated March 2009.

To determine the extent to which DHS has developed a reliable schedule for its proposed system solution, we analyzed the SBI*net* integrated master schedule as of June 2009 against the nine key schedule estimating practices in our *Cost Estimating and Assessment Guide*.[1] In doing so, we used commercially available software tools to determine whether it, for example, included all critical activities, a logical sequence of activities, and reasonable activity durations. Further, we observed a demonstration of the

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

schedule in June 2009 provided by contractor officials responsible for maintaining the schedule and program officials responsible for overseeing the contractor. In July 2009, we observed a demonstration of the program office's efforts to reconcile the version of the integrated master schedule that is exported for the government's use with the version of the schedule that the prime contractor uses to manage the program. During this demonstration, we discussed some of our concerns regarding the integrated master schedule with program officials and we inquired about deviations from some of the key practices. Subsequently, the program office provided us with a revised version of the integrated master schedule as of August 2009, which we analyzed. In doing so, we repeated the above described steps. Further, we characterized the extent to which the revised schedule met each of the practices as either Not Met, Minimally Met, Partially Met, Substantially Met, or Met.[2] In addition, we analyzed changes in the scheduled Block 1 deployment dates presented at each of the monthly program reviews for the 1-year period beginning in December 2008 and ending in November 2009.

To determine the extent to which DHS has demonstrated the cost-effectiveness of the proposed solution, we evaluated the reliability of the Block 1 life cycle cost estimate and the definition of expected system benefits, both of which are addressed below.

- *Cost estimate:* We first observed a demonstration of the cost model used to develop the estimate, which was provided by the contractor officials who are responsible for maintaining it and the program officials who are responsible for overseeing the contractor. We then analyzed the derivation of the cost estimate relative to 12 key practices associated with four characteristics of a reliable estimate. As defined in our Cost Estimating and Assessment Guide,[3] these four characteristics are comprehensive, well-documented, accurate, and credible, and the practices address, for example, the methodologies, assumptions, and source data used. We also interviewed program officials responsible for the cost estimate about the estimate's derivation. We then characterized the extent to which each of the four characteristics was met as either Not Met, Minimally Met,

[2]"Not Met" = DHS provided no evidence that satisfies any portion of the criterion. "Minimally Met" = DHS provided evidence that satisfies less than one-half of the criterion. "Partially Met" = DHS provided evidence that satisfies about one-half of the criterion. "Substantially Met" = DHS provided evidence that satisfies more than one-half of the criterion. "Met" = DHS provided complete evidence that satisfies the entire criterion.

[3]GAO-09-3SP, 8-13.

Partially Met, Substantially Met, or Met.[4] To do so, we scored each of the 12 individual key practices associated with the four characteristics on a scale of 1-5 (Not Met = 1, Minimally Met = 2, Partially Met = 3, Substantially Met = 4, and Met = 5), and then averaged the individual practice scores associated with a given characteristic to determine the score for that characteristic.

- *Benefits:* We interviewed program officials to identify any forecasts of qualitative and quantitative benefits that the system was to produce. In this regard, we were directed to the SBI*net* Mission Need Statement dated October 2006, which we analyzed. In addition, we reviewed our prior reports on the Secure Border Initiative (SBI), including a report on the SBI expenditure plan, which is a plan that DHS has been required by statute to submit to the House and Senate Appropriations Committees to, among other things, identify expected system benefits. We also interviewed program officials to determine the extent to which the system's life cycle costs and expected benefits had been analyzed together to economically justify DHS's proposed investment in SBI*net*.

  To determine the extent to which DHS has acquired its proposed system solution in accordance with key life cycle management processes, we focused on three key processes: the system engineering approach, requirements development and management, and risk management, each of which is addressed below.

- *Systems engineering approach:* We compared the program's defined system engineering approach, as defined in the SBI*net* Systems Program Office's (SPO) Systems Engineering Plan, to DHS and other relevant guidance.[5] To determine the extent to which the defined systems engineering approach had been implemented, we focused on two major "gates" (i.e., life cycle milestone reviews)—the CDR and the Deployment Readiness Review. For each of these reviews, we compared the package of documentation prepared for and used during these reviews to the program's defined system engineering approach as specified in the

[4]"Not Met" = DHS provided no evidence that satisfies any portion of the criterion. "Minimally Met" = DHS provided evidence that satisfies less than one-half of the criterion. "Partially Met" = DHS provided evidence that satisfies about one-half of the criterion. "Substantially Met" = DHS provided evidence that satisfies more than one-half of the criterion. "Met" = DHS provided complete evidence that satisfies the entire criterion.

[5]Department of Homeland Security, *DHS Acquisition Instruction/Guidebook #102-01-001*, *Appendix B*, *Systems Engineering Life Cycle*, Interim Version 1.9 (Nov. 7, 2008); and *IEEE Standard for Application and Management of the Systems Engineering Process*, IEEE Std. 1220-2005 (New York, N.Y., Sept. 9, 2005).

Systems Engineering Plan to determine what, if any, deviations existed. We also interviewed program officials as to the reason for any deviations.

- *Requirements development and management:* We compared relevant requirements management documentation, such as the Requirements Development and Management Plan, the Requirements Management Plan, the Configuration and Data Management Plan, the Operational Requirements Document, the system-level requirements specification,[6] and the component-level requirements specifications,[7] to relevant requirements development and management guidance[8] to identify any variances, focusing on the extent to which requirements were properly baselined, adequately defined, and fully traced. With respect to requirements baselining, we compared the component and system requirements as of September 2008, which were approved during the CDR that concluded in October 2008, to the component and system requirements as of November 2008, and identified the number and percentage of requirements changes. We also interviewed program officials as to the reasons for any changes. For requirements definition, we assessed the extent to which operational requirements that were identified as poorly defined in November 2007 had been clarified in the Operational Requirements Document, Elements Applicable to Block 1 System, dated November 2008. In doing so, we focused on those operational requirements that are associated with Block 1. We also traced these Block 1 operational requirements to the lower-level system requirements (i.e., system and component requirements) to determine how many of the lower-level requirements were associated with any unchanged operational requirements. For requirements traceability, we randomly selected a sample of 60 requirements from 1,008 component requirements in the program's requirements management tool, known as the Dynamic Object-Oriented Requirements System (DOORS), as of July 2009. Before doing so, we reviewed the quality of the access controls for the database, and we interviewed program and contractor officials and received a DOORS tutorial to understand their respective roles in requirements management and development and the use of DOORS. Once satisfied as to the reliability of the data in DOORS, we then traced each of the 60 requirements

[6]The SPO refers to the system-level requirements specification as the "System of System A-Level Specification."

[7]The SPO refers to the component-level requirements specifications as the "B-2" specifications.

[8]Software Engineering Institute (SEI), Capability Maturity Model Integration (CMMI®) for Acquisition, Version 1.2 (Pittsburgh, Penn., November 2007).

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 population. We used statistical methods appropriate for audit compliance testing to estimate 95 percent confidence intervals for the traceability of requirements in our sample.

- *Risk management:* We reviewed relevant documentation, such as the SBI*net* Risk/Issue/Opportunity Management Plan, the SBI*net* SPO Risk/Issue/Opportunity Management Process, and the SBI*net* Risk Management Policy, as well as extracts from the SBI*net* risk management database and minutes of meetings and agendas from the Risk Management Team and the Joint Risk Review Board. In doing so, we compared the risk management process defined in these documents to relevant guidance[9] to determine the extent to which the program has defined an effective risk management approach. Further, we observed a demonstration of the risk database, and we compared SBI*net* risks identified by us and others, including the SBI Executive Director, to the risks in the database to determine the extent to which all key risks were being actively managed. Further, we discussed actions recently taken and planned to improve risk management with the person responsible for SBI*net* risk management. We also reviewed briefings and related material provided to DHS leadership during oversight reviews of SBI*net* and interviewed program officials to ascertain the extent to which program risks were disclosed at these reviews and at meetings with congressional committees. In this regard, we also asked cognizant staff with the House Homeland Security Committee about the extent to which program risks were disclosed by program officials in status briefings.

  To determine the extent to which DHS has addressed our prior SBI*net* recommendations, we focused on the eight recommendations that we made in our September 2008 report.[10] For each recommendation, we leveraged the work described above, augmenting it as necessary to determine any plans or actions peculiar to a given recommendation. For example, to determine the status of efforts to address our prior recommendation related to SBI*net* testing, we reviewed key testing

[9]SEI, CMMI® for Acquisition, Version 1.2 (Pittsburgh, Penn., November 2007).

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

documentation, such as the Test and Evaluation Master Plan; SBI*net* component and system qualification test plans, test procedures, and test reports; program management reviews; program office briefings; and DHS Acquisition Review Board decision memoranda. We also interviewed program officials.

To support our work across the above objectives, we also interviewed officials from the Department of Defense's Defense Contract Management Agency, which provides contractor oversight services, to understand its reviews of the contractor's integrated master schedule, requirements development and management activities, risk management practices, and testing activities. We also reviewed Defense Contract Management Agency documentation, such as monthly status reports and reports pertaining to the integrated master schedule and cost reporting.

To assess the reliability of the data that we relied on to support the findings in the report, we reviewed relevant program documentation to substantiate evidence obtained through interviews with knowledgeable agency officials, where available. We determined that the data used in this report are sufficiently reliable. We have also made appropriate attribution indicating the sources of the data used.

We performed our work at the Customs and Border Protection (CBP) headquarters and contractor facilities in the Washington, D.C., metropolitan area and at a contractor facility and a Defense Contract Management Agency office in Huntsville, Alabama. We conducted this performance audit from December 2008 to May 2010 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

April 19, 2010

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-10-340, Secure Border Initiative: DHS Needs to Reconsider Its Proposed Investment in Key Technology Program (GAO Job Code 310673)

The Department of Homeland Security (Department/DHS) appreciates the opportunity to review and comment on the draft report referenced above. The U.S. Government Accountability Office (GAO) makes twelve recommendations and, with two partial exceptions, we agree with them. The first eleven recommendations are addressed to U.S. Customs and Border Protection (CBP) officials and the last one to the Department.

The GAO was asked to determine the extent to which the Department has (1) defined the scope of its proposed SBI*net* solution, (2) developed a reliable schedule for this solution, (3) demonstrated the cost effectiveness of this solution, and (4) acquired the solution using key management processes.

Over the last several months the Secretary and CBP officials have publicly indicated the need to take another, more deliberative look at the case for SBI*net* deployment. The Secretary's recently directed assessment (described below) reinforces, strengthens, and expands on that need.

In the September 2008 report ("Secure Border Initiative: DHS Needs to Address Significant Risks in Delivering Key Technology Investment" (GAO-08-1086)), the GAO identified a range of management weaknesses and program risks facing SBI*net* Block 1 deployment to Arizona. Those findings were consistent with CBP's conclusions about the state of the SBI*net* program. Beginning in August 2008, CBP and DHS implemented more rigorous oversight of planned SBI*net* acquisition, development, testing, and deployment activities. In this process SBI*net* was required at specified milestones to report its progress to the Department's Acquisition Review Board (ARB), and receive approval before continuing with the next deployment increment. The ARB completed a series of reviews to establish and baseline the technical and programmatic way ahead for the SBI*net* program. Between September 2008 and May 2009, the ARB issued three

www.dhs.gov

Acquisition Decision Memorandums (ADM) approving milestone attainment and SBI*net* deployment to portions of Arizona. The next Acquisition Decision Event (ADE-3) for SBI*net* is to occur after Tuscon-1 (TUS-1) and Ajo-1 (AJO-1) complete operational testing.

At the same time, the SBI*net* program office began taking stronger steps to improve the overall management of the effort. Initial focus areas included, among others, earned value management, risk management, schedule management, requirements management, and test discipline. CBP officials have made significant progress but the Department including CBP acknowledges that the work is not complete. In fact, correcting the weaknesses identified both by the GAO and by CBP teams are significant undertakings and will not be completed quickly. CBP officials are taking incremental steps based on their assessments of which areas are most critical to the program. The Department appreciates GAO's acknowledgement in the draft report that CBP has initiated many corrective actions.

Since last year, CBP and the Department have been re-thinking the investment strategy not only with respect to SBI*net*, but other alternative technologies as well. In January 2010, the Secretary directed a department-wide assessment of the SBI*net* program that includes an analysis of other potential alternatives for addressing security on the southwest border. The Secretary's decision was motivated by continuing delays in the development and deployment of SBI*net* capabilities, questions about the long-term viability of the program and a concern that the SBI*net* system had not yet been adequately justified by a quantitative assessment of cost and benefit.

The goal of the SBI*net* assessment is to review and assess near and long-term requirements and technology solutions to enhance border security. In the near-term assessment, the Department will identify areas of the border where deployment of technology is required earlier than SBI*net* deployments could occur. For those areas, the Department plans to procure readily available technologies—like individual cameras or Mobile Surveillance Systems to provide needed capability relatively quickly. The Department has redeployed $50 million in American Recovery and Reinvestment Act of 2009 funds originally programmed to support SBI*net* Block 1 to these readily available technologies. In the longer-term assessment, the Department plans to conduct a comprehensive, science-based SBI*net* Block-1 analysis of alternatives (AoA) to evaluate the appropriateness (as it relates to cost and mission effectiveness) of SBI*net* deployment in areas identified and prioritized by the Office of the Border Patrol along the Southwest border. The results of the AoA will aid in ensuring that SBI*net* is utilizing the most efficient and effective technological and operational solutions in all border security efforts. If this analysis suggests that the current, proven SBI*net* capabilities will significantly increase border security and are worth the cost relative to other alternatives, the Department will aggressively pursue the deployment of those capabilities. If the analysis suggests that some modifications of the current technology at different sectors of the border would enhance security, accelerate deployment, or lower the cost, then the Secretary will direct changes as necessary. If the analysis suggests that alternative technology options represent the best balance of capability and cost-effectiveness, then the Secretary will begin the process of `redirecting resources currently allocated to border security efforts to such stronger and more cost-effective options. Regardless, the decisions will be based on solid, objective analysis.

The recommendations and planned corrective actions follow.

Recommendation 1:

To address the considerable risks and uncertainties facing DHS on its SBI*net* program, GAO recommended that the Secretary direct the Commissioner of CBP to limit future investment in the program to only work that meets ***one of*** (GAO provided clarification on the recommendation sentence preceding the conditions. The words "one of" were inadvertently omitted.) the following two conditions: (1) is already under contract and supports deployment, acceptance, and operational evaluation of only those Block 1 capabilities (functions and performance levels) that are currently targeted for TUS-1 and AJO-1; or (2) provides the analytical basis for informing a Departmental decision as to what, if any, expanded investment in SBI*net*, both in terms of capabilities (functions and performance) and deployment locations, represents a prudent, responsible, and affordable use of resources for achieving the Department's border security and immigration management mission.

CBP Response:

CBP concurs. An assessment of the SBI*net* program is being conducted and funding for SBI*net* Block 1 has been frozen beyond the initial deployments to TUS-1 and AJO-1 until the assessment is completed. The assessment has near-term and a long-term phase. The near-term assessment will identify areas of the border where deployment of technology is required earlier than SBI*net* could be ready. CBP and the Department will consider procurement of already-existing systems—like individual cameras or Mobile Surveillance Systems—that could provide needed capability relatively quickly. The long-term assessment will continue to evaluate the progress of SBI*net*. The Secretary will evaluate SBI*net* initial deployment tests and analysis of alternatives to determine if it makes sense to authorize future SBI*net* deployments, and, if so, where. The decision on future deployments would be made at Acquisition Decision Event-3 (ADE-3), which will occur after TUS-1 and AJO-1 operational testing.

Department and CBP officials believe the intent of this recommendation has been satisfied and the recommendation should be considered closed.

With respect to the first condition, GAO further recommended [see recommendations 2-6] that the Secretary direct the Commissioner of CBP to have the SBI Executive Director make it a program priority to ensure that

Recommendation 2-- the integrated master schedule for delivering Block 1 capabilities to TUS-1 and AJO-1 is revised to address the key schedule estimating practices discussed in this report;

CBP Response:

CBP partially concurs. CBP acknowledges the merits of GAO's key schedule estimating and management practices described in the draft report. CBP is committed to adopting and deploying these practices for the full SBI portfolio of projects. In fact, the SBI program is making significant progress in effecting these "best practices" for the SBI*net* program. Challenges with the current contract structure (e.g., creating linkages between multiple Task Orders, significant degree of Level of Effort tasks) and "legacy" work breakdown structure (e.g.,

workbreak down structure is not product oriented and has not been updated to reflect the program's substantial evolution) will preclude CBP from fully implementing this recommendation before completion of the remainder of the TUS-1 and AJO-1 deployment effort. Nonetheless, CBP is taking the appropriate steps to improve the completeness and utility of the TUS-1 and AJO-1 schedules; these improvements will be introduced into the schedules over the next several months. The estimated completion date is May 2011.

Recommendation 3-- the currently defined Block 1 requirements, including key performance parameters, are independently validated as complete, verifiable, and affordable and any limitations found in the requirements are addressed;

CBP Response:

CBP concurs. One of the program "lessons learned" has been that the existing SBI*net* Block 1 requirements were not the most effective representation of system needs. Nonetheless, given the fact that they are the currently defined requirements, CBP personnel have focused efforts on tightening their requirements management process. CBP has also recognized the fact that their requirements allocation and flow down is incomplete or ambiguous in some areas, and that those gaps increase risk to their verification and validation plans. CBP management is continuing their effort to improve in this area. Block 1 requirements are being verified through a number of increasingly comprehensive tests such as component qualification tests, functional qualification tests, and system qualification tests. Key performance parameters have been validated through modeling as well as actual data taking with the Playas test facility. Final verification and identification of limitations will occur during System Acceptance Testing and subsequent Operational Test & Evaluation activities. Affordability will be one of the key considerations during the Department-wide assessment described above. The estimated completion date is June 2011.

Recommendation 4-- the Systems Engineering Plan is revised to include or reference documentation templates for key artifacts required at milestone gate reviews;

CBP Response:

CBP concurs. The GAO was provided a copy of the currently approved version of the Systems Engineering Plan (SEP) dated November 24, 2008. SBI*net* is managing Block 1 to the current SEP. As discussed with the GAO, the current version was written in anticipation of Block 2 and subsequent future Blocks. The next revision of the SEP will occur only if the DHS Acquisition Decision Event-3 approves further deployment of SBI*net* technology. Should the SEP be updated it will include or reference documentation templates for key artifacts required at milestone gate reviews. The completion date will be determined by the Secretary's Assessment and/or the ADE-3.

Recommendation 5-- all parent requirements that have been closed are supported by evidence of the closure of all corresponding and associated child requirements;

CBP Response:

CBP concurs. All parent requirements that have been previously closed are being reassessed to ensure the proper closure and documentation of associated child requirements. The estimated completion date is May 2010.

Recommendation 6-- all significant risks facing the program are captured, mitigated, tracked, and periodically reported to DHS and congressional decision makers.

CBP Response:

CBP concurs. As noted above, risk management has been an area of program focus for the last several months. SBI*net*'s initial efforts focused on improving the contractor's risk management processes. These risks are captured and tracked, and mitigation strategies and actions are discussed at weekly SBI*net* Risk Review Board meetings. Significant SBI*net* risks are briefed at the monthly Joint Program Review Meeting and reported each month to DHS via the Next Generation Program Reporting System (nPRS). More recent efforts have focused on adding management of SBI program risks that are NOT necessarily within the purview or influence of the contractor. These SBI risks and mitigation strategies are documented and tracked by the SBI Program Office and periodically briefed to DHS and Congressional decision makers.

Department and CBP officials believe the intent of this recommendation has been satisfied and request closure of the recommendation.

Recommendation 7:

With respect to the first condition, GAO reiterated their prior recommendations, as stated in the September 2008 report "Secure Border Initiative: DHS Needs to Address Significant Risks in Delivering Key Technology Investment" (GAO-08-1086), relative to establishing program commitments, implementing the Systems Engineering Plan, defining and managing requirements, and testing.

CBP Response:

CBP partially concurs. While the GAO recommendations reflect normal "best practices" for sound program management, the program commitments and plans have changed a great deal since the earlier GAO reports. SBI*net*'s immediate scope for initial deployment of Block 1 is now narrowed to TUS-1 and AJO-1. As noted above, CBP is making incremental improvements in each of the areas highlighted by the GAO. The Secretary will make a decision on future SBI*net* Block 1 deployments after the alternative of analysis assessment is completed, and TUS-1 and AJO-1 operational tests results have been reviewed. Consistent with DHS Acquisition Decision Memoranda 2, CBP will present comprehensive plans and cost estimates at the next ADE-3 as well as an updated program baseline for continuing the Block 1 program if that is the conclusion of the review. The estimated completion date will be determined by the Secretary's Assessment and/or the ADE-3.

With respect to the second condition, GAO recommended [recommendations 8-11] that the Secretary direct the Commissioner of CBP to have the SBI Executive Director make it a program priority to ensure that

Recommendation 8-- a life cycle cost estimate for any incremental block of SBI*net* capabilities that is to include capabilities and cover locations beyond those associated with the TUS-1 and AJO-1 deployments is developed in a manner that reflects the four characteristics of a reliable estimate discussed in this report;

CBP Response:

CBP concurs. Consistent with prior DHS Acquisition Decision Memoranda provided for the SBI*net* program, CBP will present comprehensive plans and cost estimates, as well as an updated program baseline, at the next SBI*net* Block 1 ADE-3 for continuing the Block 1 program beyond TUS-1 and AJO-1 deployments. ADE-3 will only occur if the analysis of alternatives assessment, and TUS-1 and AJO-1 operational tests validate that expanded investment in SBI*net* Block 1 makes sense and is cost efficient. Completion will be determined by the Secretary's Assessment and/or the ADE-3.

Recommendation 9-- a forecast of the qualitative and quantitative benefits to be derived from any such incremental block of SBI*net* over its useful life, or reasons why such forecasts are not currently possible, are developed and documented;

CBP Response:

CBP concurs. Consistent with prior DHS Acquisition Decision Memoranda provided for the SBI*net* program, CBP will present comprehensive plans and cost estimates, as well as an updated program baseline, at the next SBI*net* Block 1 Acquisition Decision Event-3 for continuing the Block 1 program beyond TUS-1 and AJO-1 deployments. The planned AoA will represent an initial view of both qualitative and quantitative benefits of the program. However, a more complete assessment will depend on experience with the system, data gathering, and data analysis. The analysis will also change as other factors change—like, for example, concepts of operation and migration of cross-border traffic. It is not possible to attribute a specific amount of border control just to technology—much less to SBI*net*, which is a subset of the larger technology program. Over time, however, it is possible to correlate technology with changes in border security, and to use those analyses to advise future cost / benefit analyses. CBP intends for these types of analyses to continue indefinitely. The completion date will be determined by the Secretary's Assessment and/or the ADE-3.

Recommendation 10-- the estimated life cycle costs and benefits and associated net present value of any such incremental block of SBI*net* capabilities, or reasons why such an economic analysis cannot be performed, are prepared and documented;

CBP Response:

CBP concurs. Consistent with prior DHS Acquisition Decision Memoranda provided for the SBI*net* program, CBP will present comprehensive plans and cost estimates, as well as an updated program baseline at the next SBI*net* Block 1 ADE-3. Additional deployments of SBI*net* Block 1 and investments in subsequent blocks will only occur if the assessment directed by the Secretary, and TUS-1 and AJO-1 operational tests validate that additional investments make sense. The estimated completion date will be determined by the Secretary's Assessment and/or the ADE-3.

Recommendations 11-- the results of these analyses, or the documented reasons why such analyses cannot be provided, are provided to the Commissioner of CBP and the DHS Acquisition Review Board.

CBP Response:

CBP concurs. Consistent with prior DHS Acquisition Decision Memoranda provided for the SBI*net* program, CBP will, at the next SBI*net* Block 1 ADE-3, present comprehensive plans and cost estimates as well as an updated program baseline. Additional deployments of SBI*net* Block 1 will only occur if the assessment directed by the Secretary and TUS-1 and AJO-1 operational tests validate that additional investments make sense. The results of ADE-3, including all supporting documentation, will be provided to the CBP Commissioner and the DHS Acquisition Review Board. The estimated completion date will be determined by the Secretary's Assessment and/or the ADE-3.

Recommendation 12:

With respect to the second condition, GAO recommended that the Secretary direct the Deputy Secretary of Homeland Security, as the Chair of the DHS Acquisition Review Board, to (1) decide, in consultation with the board and Commissioner of CBP, what, if any, expanded investment in SBI*net*, both in terms of capabilities (functions and performance) and deployment locations, represents a prudent, responsible, and affordable use of resources for achieving the department's border security and immigration management mission; and (2) report the decision, and the basis for it, to the department's authorization and appropriations committees.

Response:

The Secretary became uniquely aware of the promises that had been made about SBI*net* and the shortfalls it has faced during her tenure as the Governor of Arizona. Upon her appointment as Secretary of DHS, she took a hard look at the Department's progress with SBI*net* and gave the then current team at CBP a fair chance to prove that they were on the right track.

In late 2009 the Secretary directed the then-Acting Commissioner to provide his assessment of the path forward for SBI*net* and based upon the results of his review, ordered a Department-wide reassessment of the program to determine if there are alternatives that may more efficiently, effectively and economically meet our nation's border security needs.

The Department-wide review is motivated by two major considerations. The first is that continued and repeated delays in the deployment of the first sectors of SBI*net* raise fundamental questions about SBI*net*'s viability and availability to meet the ultimate need for technology along the border.

The second is that the high and growing cost of SBI*net* obligates this administration to conduct a full and comprehensive analysis of alternative options to ensure the Department is maximizing the impact and effectiveness of the substantial taxpayer resources being devoted to border security technology. This type of comprehensive analysis of alternatives was not undertaken prior to initiating the program. Since the inception of the SBI*net* program, and since the beginning of the Secretary's tenure, DHS has significantly enhanced the review and approval processes for its major acquisition programs. The Secretary has now directed the application of that process to re-assess the value of this program.

The assessment is being led by the Department's Office of Management in conjunction with CBP and the Science and Technology Directorate. The assessment has an immediate, near-term and a long-term phase.

The immediate phase was necessary to address concerns over Recovery Act funding. This phase concluded on March 16 when Department officials announced that they would be redirecting $50 million in Recovery Act funds that were scheduled to be spent on SBI*net* to alternative technology projects that will immediately improve the Department's ability to secure the U.S.-Mexico border.

In the near-term phase, Department and CBP officials will review currently available technology options, including SBI*net* Block 1 and others such as remote-controlled camera systems called Remote Video Surveillance Systems truck-mounted systems with cameras and radar called Mobile Surveillance Systems, thermal imaging devices, ultra-light detection, backscatter units, mobile radios, and cameras and laptops for pursuit vehicles, to determine if the Department needs to redirect already enacted SBI*net* funds to other proven solutions to meet urgent needs, as identified by the Office of Border Patrol (OBP), within the Arizona portion of the Southwest Border.

In the long-term phase, Department and CBP officials will conduct a comprehensive, science-based SBI*net* Block 1 AoA to evaluate the appropriateness, as it relates to cost and mission effectiveness, of SBI*net* deployment in areas identified and prioritized by OBP along the Southwest Border. The results of the AoA will aid in ensuring Department personnel are employing the most efficient and effective technological and operational solutions in all border security efforts. If this analysis suggests that the current, proven capabilities of SBI*net* will significantly increase border security and are worth the cost relative to other alternatives, the Department will aggressively pursue its deployment. If the analysis suggests that some modifications of the current technology at different sectors of the border would enhance security, accelerate deployment or lower cost, then the Secretary will direct changes as necessary. If the analysis suggests that alternative technology options represent the best balance of capability and cost-effectiveness, then the Secretary will begin redirecting resources currently allocated for border security efforts to such stronger and more cost effective options. Regardless, the

decisions will be based on solid, objective analysis. Furthermore, future deployment decisions will be informed by the Administration's continued refinement of border strategies and desired outcomes. The alternatives developed for use in the AoA will need to be informed by these processes, as available, and be distributed across a sufficient range to ensure relevance to these processes to develop greater clarity on strategic questions like level of effort and prioritization across threats.

As part of the assessment officials are reaching outside of the Department, to ensure that management has a chance to review ideas from other sources. We will look forward to continued discussion with the Congress as part of that process.

Sincerely,

Jerald E. Levine
Director
Departmental GAO/OIG Liaison Office

Appendix III: Status of Key GAO Recommendations

In September 2008, we reported on a number of SBI*net* program management weaknesses and associated risks related to establishing program commitments, developing an integrated master schedule, defining and implementing a life cycle management approach, developing and managing requirements, and testing. To address these weaknesses and risks, we made a number of recommendations. Table 7 provides details on DHS efforts to address each recommendation.[1]

Table 7: Status of DHS Implementation of Key GAO Recommendations

Recommendation	DHS comment	Status	GAO analysis
(1/2) Ensure the risks associated with planned SBI*net* acquisition, development, testing, and deployment activities are immediately assessed and the results, including proposed alternative courses of action for mitigating the risks, are provided to DHS's senior leadership, as well as to the department's congressional authorization and appropriation committees.	Concurred	Not implemented	The SBI*net* Program Office (SPO) did not immediately assess key risks facing the program and brief key decision makers. According to agency documentation, shortly after receiving our draft report, the SPO met with the DHS Acquisition Review Board to formally discuss program risks and agree on courses of action to best mitigate them. However, the briefing slides from the meeting do not identify risks and alternative courses of action to mitigate them. Instead, the briefing contained one slide that identified factors contributing to changes in the program's schedule. Further, the SPO has yet to formally capture a number of acquisition risks such as lack of staff with appropriate acquisition expertise, lack of formalized acquisition processes, problems with the integrated master schedule and earned value management (EVM)[a] reporting, and lack of agreement on key performance parameters. The SPO also could not demonstrate that it briefed the key congressional committees regarding the risks facing the program or specific mitigation plans. While program officials stated that they briefed congressional committees during the fall of 2008, which they said included disclosure of risks, these officials did not have any documentation to show when these briefings occurred, who was present, and whether or not program risk was a topic of discussion. Further, House Homeland Security Committee staff told us that while they received several briefings on SBI*net* during the fall of 2008, they were not specifically briefed on program risks.

[1] GAO-08-1086.

Recommendation	DHS comment	Status	GAO analysis
(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 establish when these capabilities are to be deployed and are to be operational.	Concurred	Partially implemented	The SPO has established and baselined program commitments, including the system's functional and performance capabilities to be deployed and the timing of their deployment and operational use. However, these commitments have continued to decrease. For example, the SPO has defined the capabilities to be deployed in the Tucson and Yuma Sectors; however, it dropped the El Paso Sector from its Block 1 deployment plans. Further, the functional capabilities for Block 1 have also been reduced. Specifically, the number of component-level requirements for Block 1 has decreased by about 32 percent since they were baselined in late 2008. In addition, system performance has been reduced. For example, the system is now only required to achieve a 49 percent probability of identifying items of interest that cross the border. Moreover, a time frame for when these capabilities are to be deployed and begin operating continues to be delayed, and is still uncertain. To illustrate the extent of changes to schedule commitments, as of July 2008, program officials stated that the deployments to the Tucson Border Patrol Station (TUS-1) and the Ajo Border Patrol Station (AJO-1) would be operational "sometime" during 2009. However, August 2009 documentation shows that TUS-1 and AJO-1 were scheduled for acceptance by the government in February 2010 and July 2010, respectively. Moreover, the SBI Executive Director stated in December 2009 that the entire Block 1 schedule is being reviewed and revised because of uncertainties with projected completion dates. Further, as of February 2010, TUS-1 and AJO-1 are proposed to be accepted in September 2010 and November 2010, respectively. However, this proposed schedule has yet to be approved by CBP. Finally, the program's cost commitments are not based on complete, current, or reliable estimates. The Block 1 life cycle cost estimate does not cover all costs, has not been updated to reflect changes to the program, and does not otherwise sufficiently address leading best practices for cost estimating, such as properly identifying the ground rules and assumptions used to estimate costs, using an independent cost estimate to verify the estimate's validity, and undergoing risk and uncertainty analysis.

Recommendation	DHS comment	Status	GAO analysis
(4) Finalize and approve an integrated master schedule that reflects the timing and sequencing of the work needed to achieve these commitments.	Concurred	Partially implemented	The SPO finalized an integrated master schedule for SBI*net*, and DHS approved the schedule in March 2009. However, the schedule is not reliable because it does not adequately comply with key practices for schedule estimation, as discussed in this report. For example, the schedule does not capture all activities as defined in the work breakdown structure or integrated master plan. Specifically, 57 percent of the activities listed in the work breakdown structure (71 of 125) and 67 percent of the activities listed in the integrated master plan (46 of 69) were not in the integrated master schedule. In particular, the schedule is missing efforts associated with systems engineering, sensor towers, logistics, system test and evaluation, operations support, and program management. Further, the schedule does not include key activities to be performed by the government. While the schedule shows the final activity in the government process for obtaining an environmental permit in order to construct towers, it does not include the related government activities needed to obtain the permit. In addition, the schedule does not reflect a valid critical path. For example, it is missing government and contractor activities, and is thus not complete, and it is missing some predecessor links, and improperly establishes other predecessor and successor links.
(5) Revise and approve versions of the SBI*net* life cycle management approach, including the draft Systems Engineering Plan (SEP) and draft Test and Evaluation Management Plan (TEMP), and in doing so, ensure that these revised and approved versions are (a) consistent with one another, (b) reflect program officials' recently described changes to the engineering and testing approaches, and (c) reflect relevant federal guidance and associated leading practices.	Concurred	Partially implemented	(a) The SEP and TEMP were revised and approved in November 2008, and these documents are largely consistent with one another. (b) The SEP and TEMP reflect the program officials' described changes to its engineering and testing approaches. (c) The revised SEP and TEMP reflect many aspects of relevant guidance and leading practices, as discussed in this report. For example, the SEP defines a number of gate reviews to guide system development and operations, such as initial planning reviews, requirements reviews, system design reviews, and test reviews. In addition, it requires key artifacts and program documents identified in DHS guidance, such as a concept of operations, an operational requirements document, a deployment plan, a risk management plan, a life cycle cost estimate, requirements documentation, and test plans. However, the SEP does not address the content of the key artifacts that it requires. For example, it does not provide a sample document or content template for the required documents, such as the concept of operations, the operational requirements document, or a deployment plan. Furthermore, the TEMP, while consistent with some aspects of relevant guidance, still has limitations. For example, and as discussed in more detail below, the TEMP describes the program's test strategy, scope, and resource requirements, but does not adequately define roles and responsibilities and provide sufficient detail for key testing and management activities.

Recommendation	DHS comment	Status	GAO analysis
(6) Ensure that the revised and approved life cycle management approach is fully implemented.	Concurred	Partially implemented	Program officials stated that they have yet to fully implement the Systems Engineering Plan. As a result, they have not consistently implemented the plan when conducting gate reviews for life cycle activities. For example, while the SPO reviewed and considered all but one of the key artifacts for the TUS-1 Deployment Readiness Review that concluded in April 2009, a number of key documents were not reviewed during the CDR, including the quality plan, security test plan, and plans for testing, training, and system maintenance. According to program officials, this was because the contractor is required to follow criteria in the task order, which was written prior to the CDR. Program officials stated that they are working to bring the task orders into alignment with the revised SEP.
(7) Implement key requirements development and management practices to include (a) baselining requirements before system design and development efforts begin; (b) analyzing requirements prior to being baselined to ensure that they are complete, achievable, and verifiable; and (c) tracing requirements to higher-level requirements, lower-level requirements, and test cases.	Concurred	Partially implemented	(a) A baseline set of requirements for the TUS-1 and AJO-1 system deployments were established in October 2008. Baselined requirements associated specifically with the Network Operations Center/Security Operations Center (NOC/SOC) were not adequately defined at this time, as evidenced by the fact that about 43 percent of these requirements were significantly changed 2 months later. (b) Twelve of Block 1's 69 operational requirements are not yet complete, achievable, verifiable, or affordable. The 12 operational requirements, which were reported as deficient by DHS in November 2007, are associated with 16 system-level requirements, which in turn are linked to 152 component-level requirements, which represent approximately 15 percent of the total number of component-level requirements. Program officials stated that they planned to address the problems with requirements during testing. However, they also told us that unclear and ambiguous requirements contributed to numerous and extensive rewriting of test cases. As we recently reported,[b] most SBI*net* system qualification and component qualification test cases had to be rewritten extemporaneously during test execution, in part because of differing opinions among staff about what was required to effectively test and satisfy the requirements. (c) The Block 1 component-level requirements are now largely traceable backward to system and operational requirements, and forward to design requirements and verification methods.

Recommendation	DHS comment	Status	GAO analysis
(8) Implement key test management practices to include (a) developing and documenting test plans prior to the start of testing; (b) conducting appropriate component-level testing prior to integrating system components; and (c) 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.	Partially disagreed	Partially implemented	(a) Test plans and procedures were developed for component and system qualification testing; however, they were not defined in accordance with key aspects of guidance. For example, none of the 10 system and component test plans adequately described testing risks, and only 2 of the plans included quality assurance procedures for making changes to test plans during execution. In addition, a large number of test procedures were changed during test execution, and these changes were not made in accordance with documented quality assurance processes. Rather, changes were made based on an undocumented understanding that program officials said they had established with the contractor. (b) Qualification testing for 9 SBI*net* components occurred prior to qualification testing of the entire system. (c) A test management approach has been established that is consistent with some, but not all, aspects of relevant guidance. For example, the 2008 TEMP describes (1) a test management strategy that is consistent with the program's system development approach, (2) a progressive sequence of tests to verify that both individual system parts, as well as the integrated system, meet specified requirements, and (3) the staff, resources (equipment and facilities), and funding requirements associated with SBI*net* testing. However, while the TEMP includes high-level descriptions of various test documentation and reports associated with developmental and operational testing, it does not include sufficient detail to allow for key testing and oversight activities. In addition, the TEMP defines high-level roles and responsibilities for various entities related to program testing, but similar to what we reported in 2008, these responsibilities are defined in vague terms and contain errors. Further, the TEMP lacks a clear definition for how the program is to prioritize and analyze all problems discovered during testing. Specifically, while the TEMP requires that test plans include guidance for recording anomalies during testing, it does not describe a process for analyzing and prioritizing anomalies according to severity, nor does it describe a process for resolving them. Finally, although the TEMP and related SBI*net* task orders include descriptions of certain metrics, some of those metrics are not associated with desired quality outcomes and do not identify how they support specific test objectives.

Source: GAO analysis of DHS data.

[a]EVM is a management tool for monitoring a program's cost and schedule performance by measuring the value of the work accomplished in a given period, compared to the planned value of the work scheduled for that period and the actual cost of the work accomplished.

[b]GAO, *Secure Border Initiative: DHS Needs to Address Testing and Performance Limitations That Place Key Technology Program at Risk*, GAO-10-158 (Washington, D.C.: Jan. 29, 2010).

Appendix IV: Detailed Results of GAO Assessment of SBI*net* Program Schedule

Our research has identified a range of best practices associated with effective schedule estimating.[1] These are (1) capturing all activities, (2) sequencing all activities, (3) assigning resources to all activities, (4) establishing the duration of all activities, (5) integrating activities horizontally and vertically, (6) establishing the critical path for all activities, (7) identifying reasonable float time between activities, (8) conducting a schedule risk analysis, and (9) updating the schedule using logic and durations. We assessed the extent to which the SBI*net* integrated master schedule, dated August 2009, met each of the nine practices as either Not Met (the program provided no evidence that satisfies any portion of the criterion), Minimally Met (the program provided evidence that satisfies less than one-half of the criterion), Partially Met (the program provided evidence that satisfies about one-half of the criterion), Substantially Met (the program provided evidence that satisfies more than one-half of the criterion), and Met (the program provided evidence that satisfies the entire criterion). Table 8 shows the detailed results of our analysis.

Table 8: Detailed Results of SBI*net* Satisfaction of Scheduling Best Practices

Practice	Description	Met?	Results
(1) Capturing all activities	The schedule should reflect all activities (steps, events, outcomes, etc.) as defined in the program's work breakdown structure (WBS)[a] to include activities to be performed by both the government and its contractors.	Minimally	The schedule does not capture all activities as defined in the program's WBS or integrated master plan (IMP).[b] For example, 57 percent (71 of 125) of the activities listed in the WBS and 67 percent (46 of 69) of the activities listed in the IMP were not in the integrated master schedule. In particular, the schedule does not include key efforts associated with systems engineering, sensor towers, logistics, system test and evaluation, operations support, and program management. Further, the schedule only includes a few activities to be performed by the government. For example, while the schedule shows the final activity in the government process for obtaining an environmental permit in order to construct towers, it does not include the related government activities needed to obtain the permit.

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

Practice	Description	Met?	Results
(2) Sequencing all activities	The schedule should sequence activities in the order that they are to be implemented. In particular, activities that must finish prior to the start of other activities (i.e., predecessor activities) as well as activities that cannot begin until other activities are completed (i.e., successor activities) should be identified.	Substantially	The schedule identifies virtually all of the predecessor and successor activities. Specifically, only 9 of 1,512 activities (less than 1 percent) were missing predecessor links. Further, only 21 of 1,512 activities (about 1 percent) had improper predecessor and successor links. While the number of unlinked activities is very small, not linking a given activity can cause problems because changes to the durations of these activities will not accurately change the dates for related activities. More importantly, 403 of 1,512 activities (about 27 percent) are constrained by "start no earlier than" dates, which is significant because it means that these activities are not allowed to start earlier, even if their respective predecessor activities have been completed.
(3) Assigning resources to all activities	The schedule should reflect who will do the work activities, whether all required resources will be available when they are needed, and whether any funding or time constraints exist.	Minimally	The schedule does not assign the resources needed to complete the captured activities. Instead, the contractor's resource data are maintained separately as part of its EVM system and are available to the government upon request.
(4) Establishing duration of all activities	The schedule should reflect the duration of each activity. These durations should be as short as possible and have specific start and end dates.	Substantially	The schedule establishes the duration of key activities and includes specific start and end dates for most of the activities. For example, the schedule establishes reasonable durations for 1,164 of the 1,241[c] activities (about 94 percent) in the schedule. However, the remaining 77 activities (or 6 percent) are not always of short duration, with 15 of the 77 having durations that ranged from 102 to 177 days.
(5) Integrating schedule activities horizontally and vertically	The schedule should be horizontally integrated, meaning that it should link the products and outcomes associated with sequenced activities. The schedule should also be vertically integrated, meaning that traceability exists among varying levels of activities and supporting tasks and subtasks.	Partially	The schedule is not fully integrated horizontally. While horizontal integration exists between task orders for work that is under contract, the schedule does not capture all key activities in the WBS and IMP. Further, as discussed above, the schedule is missing some predecessors and improperly establishes other predecessor and successor links. The schedule is also not fully integrated vertically. While the schedule provides traceability between higher-level and lower-level schedule views, it does not capture all of the WBS and IMP activities, as noted above, and thus these activities are not integrated.
(6) Establishing the critical path for all activities	The critical path represents the chain of dependent activities with the longest total duration in the schedule.	Partially	The schedule does not reflect a valid critical path for several reasons. First, it is missing government and contractor activities, and is thus not complete. Second, the schedule does not include all predecessor links between activities, and in some cases, the predecessor and successor links are not correct. Unless all activities are included and properly linked, it is not possible to generate a true critical path. These problems were recognized by the Defense Contract Management Agency[d] as early as November 2008, when it reported that the contractor could not develop a true critical path that incorporates all program elements.

Practice	Description	Met?	Results
(7) Identifying reasonable float between activities	The schedule should identify a reasonable amount of float—the time that a predecessor activity can slip before the delay affects successor activities—so that schedule flexibility can be determined. As a general rule, activities along the critical path typically have the least amount of float.	Partially	The schedule identifies float; however, the amount of float is excessive. For example, 202 of 1,512 activities (about 13 percent) show float between 101 and 150 days, or about 3 to 5 months. Another 5 of the 1,512 activities (less than 1 percent) show float between 970 and 1,427 days (about 2.5 to almost 4 years). This high level of float is being driven by the lack of successor relationships among activities, as previously discussed, and may be due to incorrect dependencies between activities. Moreover, 138 of the 208 activities (about 85 percent) on the critical path show negative float, meaning that the activities must be completed ahead of schedule in order for the overall program to be on time. Much of the negative float in the schedule is due to a number of activities with start-no-earlier-than constraints, which means that these activities cannot start earlier even if the predecessor is complete. Program officials stated that they plan to review the need for these constraints.
(8) Conducting a schedule risk analysis	A schedule risk analysis is used to predict the level of confidence in the schedule, determine the amount of time contingency needed, and identify high-priority schedule risks.	Not	A risk analysis of the schedule's vulnerability to slippages in the completion of activities has not been performed.
(9) Updating the schedule using logic and durations	The schedule should use logic and durations in order to reflect realistic start and completion dates, be continually monitored to determine differences between forecasted completion dates and planned dates, and avoid logic overrides and artificial constraint dates.	Partially	The SPO and the contractor review the schedule during the weekly Program Management Reviews and discuss updates, confirm status and progress of activities, and document any concerns and impacts. Further, program officials stated that critical-path and near-critical-path activities are managed continuously to determine if float conditions are worsening or improving and to ensure that changes are reported to management as soon as possible. Further, the program generates several monthly reports related to the critical path, schedule metrics, and diagnostic filters that provide specific information about each task order and the program as a whole. Moreover, both SPO and contractor officials responsible for updating and monitoring the schedule have received the proper training and have experience in critical path method scheduling. Nevertheless, the schedule does not reflect a valid critical path, as discussed above. Further, problems with the predecessor and successor links, and durations also previously discussed, as well as other anomalies in the schedule, raise questions about the reliability of the activities' start and end dates. For example, 37 of 1,512 activities (about 2 percent) should have started as of August 2009, but did not, yet the schedule software did not automatically advance the start date accordingly. Further, the schedule showed 95 of 1,512 activities (about 6 percent) with actual start dates after the date of the schedule (August 2009), and 84 of 1,512 activities (about 6 percent) with actual finish dates after these dates, neither of which should be the case. In addition, 403 of 1,512 activities (about 27 percent) activities have "start no earlier than" constraints, which means that the schedule does not allow activities to start earlier, even when the predecessor has been completed.

Source: GAO analysis of DHS data.

Note: “Not Met” = DHS provided no evidence that satisfies any of the criterion. “Minimally Met” = DHS provided evidence that satisfies less than one-half of the criterion. “Partially Met” = DHS provided evidence that satisfies about one-half of the criterion. “Substantially Met” = DHS provided evidence that satisfies more than one-half of the criterion. “Met” = DHS provided complete evidence that satisfies the entire criterion.

[a]The WBS is a document that defines in detail the work necessary to complete a program’s objectives.

[b]An IMP is an event-based hierarchy of program events that must be completed to complete the program.

[c]This number of activities does not include milestones, which by definition have a duration of zero.

[d]Based on a letter of commitment with CBP, the Defense Contract Management Agency is to provide CBP with contract administration services for SBI*net*, including the identification of issues that could impact Boeing’s ability to perform the requirements in the task orders in accordance with established criteria. In this regard, the Defense Contract Management Agency provides the SPO with monthly reports that include an assessment of Boeing’s system engineering processes, the current and projected status of operational and technical issues, and the results of ongoing internal audits.

Appendix V: Detailed Results of GAO Assessment of SBI*net* Cost Estimate

Our research has identified 12 practices that are integral to effective program life cycle cost estimating.[1] These 12 practices in turn relate to four characteristics of a high-quality and reliable cost estimate:

- *Comprehensive:* The cost estimate should include all government and contractor costs over the program's full life cycle, from program inception through design, development, deployment, and operation and maintenance to retirement. It should also provide sufficient detail to ensure that cost elements are neither omitted nor double-counted, and it should document all cost-influencing ground rules and assumptions.

- *Well-documented:* The cost estimate should capture in writing things such as the source and significance of the data used, the calculations performed and their results, and the rationale for choosing a particular estimating method or reference. Moreover, this information should be captured in such a way that the data used to derive the estimate can be traced back to, and verified against, their sources. Finally, the cost estimate should be reviewed and accepted by management to demonstrate confidence in the estimating process and the estimate.

- *Accurate:* The cost estimate should not be overly conservative or optimistic, and should be, among other things, based on an assessment of most likely costs, adjusted properly for inflation, and validated against an independent cost estimate. In addition, the estimate should be updated regularly to reflect material changes in the program and actual cost experience with the program. Further, steps should be taken to minimize mathematical mistakes and their significance and to ground the estimate in documented assumptions and a historical record of actual cost and schedule experiences with other comparable programs.

- *Credible:* The cost estimate should discuss any limitations in the analysis due to uncertainty or biases surrounding data or assumptions. Major assumptions should be varied and other outcomes computed to determine how sensitive the estimate is to changes in the assumptions. Risk and uncertainty inherent in the estimate should be assessed and disclosed. Further, the estimate should be properly verified by, for example, comparing the results with an independent cost estimate.

Our analysis of the $1.3 billion SBI*net* life cycle cost estimate relative to each of the 12 best practices, as well as to each of the four characteristics,

[1]GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP (Washington, D.C.: March 2009), 8-13.

is summarized in table 9. A detailed analysis relative to the 12 practices is in table 10.

Table 9: Summary of SBI*net* Satisfaction of Cost Estimating Characteristics and Related Practices/Steps

Characteristic	Met?	Practice/step	Met?
Comprehensive	Partially	Did the team develop a well-written study plan? (Practice 2)	Partially
		Was the estimating structure determined? (Practice 4)	Partially
		Were ground rules and assumptions identified? (Practice 5)	Minimally
Well-documented	Partially	Are the cost estimate's purpose and scope defined and documented? (Practice 1)	Partially
		Were program characteristics defined? (Practice 3)	Substantially
		Were ground rules and assumptions identified? (Practice 5)	Minimally
		Were valid and useful historical data collected? (Practice 6)	Partially
		Was the estimate documented? (Practice 10)	Substantially
		Was the estimate presented to management for approval? (Practice 11)	Minimally
Accurate	Minimally	Was the point estimate developed and compared to an independent cost estimate? (Practice 7)	Minimally
		Is the estimate updated to reflect actual costs and changes? (Practice 12)	Minimally
Credible	Partially	Was a sensitivity analysis conducted? (Practice 8)	Partially
		Was a risk and uncertainty analysis conducted? (Practice 9)	Partially
		Was the point estimate developed and compared to an independent cost estimate? (Practice 7)	Minimally

Source: GAO analysis of DHS data.

Note: "Not Met" = DHS provided no evidence that satisfies any portion of the criterion. "Minimally Met" = DHS provided evidence that satisfies less than one-half of the criterion. "Partially Met" = DHS provided evidence that satisfies about one-half of the criterion. "Substantially Met" = DHS provided evidence that satisfies more than one-half of the criterion. "Met" = DHS provided complete evidence that satisfies the entire criterion.

Table 10: Detailed Results of SBI*net* Satisfaction of 12 Cost Estimating Practices/Steps

Practice	Description	Met?	Results
(1) Are the cost estimate's purpose and scope defined and documented?	A life cycle cost estimate provides a structured accounting of all resources and associated cost elements required to develop, produce, deploy, and sustain a program. As such, the estimate should include (a) a level of detail consistent with the level of detail available for the program; (b) all applicable costs, including all past (or sunk), present, and future costs for every aspect of the program, regardless of funding source; and (c) a defined scope for the estimate.	Partially	The Block 1 life cycle cost estimate of $1.3 billion does not account for all resources and cost elements associated with Block 1 development, acquisition, deployment, and sustainment. In particular: (a) The cost estimate is generally defined at a level of detail that is consistent with the WBS[a] for the program, and thus allows for the development of a quality estimate. (b) The cost estimate does not include all applicable costs. For example, the estimate excludes sunk costs, including design, development, and testing, as well as contractor and government program management and support costs. Further, it includes only 1 year of operations and maintenance costs. (c) Program officials stated that the scope of the cost estimate includes the cost to complete Block 1 as of the time of the Acquisition Program Baseline, which was approved in March 2009. However, this scope is not consistent with the estimate's stated purpose, as it excludes sunk costs and operation and maintenance costs over the system's useful life.
(2) Did the team develop a well-written study plan?	A cost estimate should be based on a written study plan that identifies, among other things (a) the estimating team's composition, (b) the subject matter experts that the estimating team will rely on for information, (c) the estimating approach, and (d) a schedule for completing the estimate that includes adequate time to perform the work.	Partially	The cost estimate was not based on a written study plan; however, it partially met other aspects of this practice. Specifically: (a) A contractor with many years of experience in government cost estimating was hired to develop the estimate. (b) The contractor had access to government subject matter experts, including program office logisticians, engineers, and technicians, as well as Border Patrol staff, for key information, such as ground rules, assumptions, and requirements for labor and material. (c) Program officials described the overall cost estimating approach and this approach largely follows relevant estimating procedures, including developing a detailed WBS, identifying cost estimating methods, identifying source data and subject matter experts for each WBS element, conducting data analysis, deriving the estimate, and performing recursive updates as data become available. (d) A schedule for completing and updating the estimate does not exist.

Practice	Description	Met?	Results
(3) Were program characteristics defined?	Critical to developing a reliable cost estimate is having an adequate understanding of the program's key characteristics (i.e., a defined technical program baseline), including documented requirements, purpose, technical characteristics, development plan, acquisition strategy, operational plan, and risk. The less such information is known, the more assumptions must be made, thus increasing the risk associated with the estimate.	Substantially	The SPO has defined and documented a technical program baseline across various documents that together describe the program's requirements, purpose, technical characteristics, development plan, acquisition strategy, operational plan, and risks. Examples of the source data for this baseline include critical design review and deployment readiness review documentation as the basis for the requirements and technical characteristics, and the Project Laydown Workbook Revision 12 as the basis for the master tower construction plan for the location, tower height, and radar and camera type.
(4) Was the estimating structure determined?	A WBS is the cornerstone of every program. It defines the detailed work elements needed to accomplish the program's objectives and the logical relationship among these elements, and it provides a systematic and standardized way for collecting data across the program. Thus, it is an essential part of developing a program's life cycle cost estimate. As such, a WBS should (a) decompose product-oriented elements to an appropriate level of detail (generally to at least three levels of decomposition) to ensure that cost elements are neither omitted nor double counted; (b) provide a standardized way for collecting data across the program; (c) be consistent across the cost estimate, integrated master schedule and EVM system;[b] (d) be updated as the program becomes better defined and to reflect changes as they occur; and (e) include a dictionary that defines each element and how it is related to others in the hierarchy.	Partially	The SPO has a WBS that defines much, but not all, of the detailed work and the relationships among work elements needed to accomplish the program's objectives. More specifically: (a) The WBS decomposes product-oriented work elements (as well as process-oriented work elements). For example, radar, camera, tower, and unattended ground sensor products are visible and decomposed to a third level of detail, thus ensuring that associated costs are neither omitted nor double counted. However, the WBS omits several key elements, such as sunk costs for contractor program management; overhead; system design, development and testing; and software design, development, and testing. Therefore, it does not fully represent all work necessary to accomplish the program's objectives. (b) The WBS and the cost estimate are standardized to a third level of decomposition. The cost estimate is further decomposed to provide greater granularity in the estimate. (c) The WBS is consistent with the cost estimate and the EVM system to the third level of decomposition. However, the WBS is not consistent with the integrated master schedule. In particular, the schedule is missing several level-2 WBS elements, including Project Sector Deployment, Logistics, Test and Evaluation, Operations Support, Program Management, and Transportation. (d) The WBS has been modified over time to reflect an updated view of the program. For example, while the WBS is decomposed to level 5 for Project Sector Acquisitions, the cost estimate further decomposes this work element to level 8 based on the availability of more detailed information. (e) The WBS includes a dictionary that defines each work element down to a third level of decomposition and its relationships with other work elements.

Practice	Description	Met?	Results
(5) Were ground rules and assumptions identified?	Cost estimates are typically based on limited information and therefore need to be bound by the constraints that make estimating possible. Among other things, these constraints, which include ground rules and assumptions, should at a minimum be identified. More specifically, (a) risks associated with assumptions should be identified and traced to WBS elements; (b) budget constraints should be identified; (c) inflation indices and their source should be identified; (d) dependencies on other organizational entities, and the effect on the estimate if the assumptions fail, should be identified; (e) items that have been excluded from the estimate should be identified, documented, and explained; (f) the effect on cost and schedule if technology maturity assumptions fail should be addressed; and (g) risk distributions for all assumptions should be determined.	Minimally	The ground rules and assumptions affecting the cost estimate were largely not identified, documented, and assessed. In particular: (a) Risk was estimated and documented for material unit prices and labor rates. However, the risk associated with the assumptions that drive the cost estimate, such as number of towers and staff and schedule variations, were not identified and traced to WBS elements. (b) Budget constraints are not identified in the cost estimate documentation. (c) The inflation rates were taken from Office of Management and Budget Circular A-94.[c] However, they were improperly derived. Specifically, the SPO overstated the inflation rate by using the projected interest rate rather than the projected inflation rate. (d) The estimate includes only contractor costs and does not recognize assumptions about, for example, government costs. (e) The estimate documents excluded costs, such as government effort, operations and maintenance costs beyond the first year of steady state support, operations and maintenance costs of legacy equipment, and participating agency support costs. Further, other excluded costs were documented in a supplemental briefing from program officials, including sunk costs, software, government program management and support costs, and costs of expected block evolutions. Also, explanations as to why these costs were excluded were not documented. (f) SBI*net* is to be largely based on commercial-off-the-shelf (COTS) products, and thus the cost estimate depends on assumptions about the maturity of these products. However, the estimate does not address the effect of the failure of these product maturity assumptions on the cost estimate. These assumptions are significant because COTS limitations have been identified as a key contributor to Block 1's reduced scope and schedule delays. (g) The estimate includes risk distributions for some, but not all, of the assumptions. The majority of these distributions were based on "industry standards" and opinions from subject matter experts (e.g., logisticians, engineers, technicians, and Border Patrol staff from various integrated product teams).

Practice	Description	Met?	Results
(6) Were valid and useful historical data collected?	Cost estimates should be rooted in historical data. To ensure that these data are applicable and useful, the following activities should be performed: (a) cost drivers should be identified; (b) data should be collected from primary sources, and the data's source, content, time, and units should be documented and their accuracy and reliability should be assessed; (c) data should be continually collected so that they are available for future use; (d) understanding of the data should include meeting with parties who are responsible for them; (e) the data should be reviewed and benchmarked for reasonableness; and (f) scatter plots and descriptive statistics should be used to analyze the data.	Partially	Cost estimates were, in part, grounded in historical data. However, key activities associated with using such data were not performed. Specifically: (a) The cost estimate did not specifically identify cost drivers. However, a supplemental briefing did identify key cost drivers. For example, the top five cost drivers for deployment were identified as land tower systems, unattended ground systems, vehicle communications upgrades, program management for deployment, and microwave transceivers and equipment, and the top five cost drivers for operations and maintenance were identified as maintenance technicians, vehicle console technicians, depot repair (normal wear and tear), camera overhaul, and depot repair (vandalism). (b) For hardware and material cost estimates, historical data were collected from Boeing primary data sources, such as technical data from design reviews, engineering drawings, technical workbooks, bills of material data, and purchase agreements. For construction labor cost estimates, data were collected from a secondary source—the Davis-Bacon National Construction estimate labor rates. For nonconstruction labor cost estimates, data were collected from Boeing (and General Services Administration) labor rates and labor hours that were estimated via engineering judgment, which is not a credible primary estimating method according to GAO best practices. Further, the documentation for these nonconstruction labor estimates did not indicate the source of the data. To assess the data's accuracy and reliability, officials told us that the estimators met with program office subject matter experts and regularly attended program management reviews, design reviews, and integrated product team meetings. (c) The SPO regularly receives Boeing EVM data. However, program officials stated that the data are not used for cost estimating. (d) The estimating team met with program office subject matter experts and regularly attended program management reviews, design reviews, and integrated product team meetings to help understand the data collected. (e) The data used were not benchmarked against relevant historical data, such as Project 28 deployment and logistics costs. (f) Scatter plots or statistical analysis were not used.

Practice	Description	Met?	Results
(7) Was the point estimate developed and compared to an independent cost estimate?	A point estimate represents the most likely estimate of costs given the underlying data, and thus it should be developed and validated. To accomplish this, (a) the WBS cost element estimates should be aggregated using a cost estimating method; (b) the estimate should be checked for accuracy, double-counting, and omissions, and it should be validated against an independent cost estimate; and (c) estimates of software costs should be based on software cost estimating best practices.	Minimally	A point estimate of $1.302 billion was developed, but it was not adequately validated. Specifically: (a) The point estimate was developed using primarily the "engineering build-up" method, with a few cost elements estimated using the "analogy" method. (b) While the use of cross-checks was limited to only a few hardware elements, no instances of double-counting were visible, and the spreadsheet calculations were accurate given the input parameters and assumptions. However, no independent cost estimate was developed. (c) Software costs were not estimated. According to program officials, these costs were considered to be outside the scope of the estimate.
(8) Was a sensitivity analysis conducted?	A sensitivity analysis examines the effects of changing assumptions and ground rules. To be useful, (a) the analysis should identify key cost drivers and their parameters and assumptions should be examined; (b) the cost estimate should be redone by varying each parameter between its minimum and maximum range; (c) the analysis should be documented, and the re-estimate should be repeated for parameters associated with key cost drivers.	Partially	A sensitivity analysis was not conducted. Specifically: (a) The cost estimate did not identify and vary most major cost drivers and their underlying assumptions and parameters. However, a supplemental briefing did identify key cost drivers. For example, the top five cost drivers for deployment are land tower systems, unattended ground systems, vehicle communications upgrades, program management for deployment, and microwave transceivers and equipment, and the top five cost drivers for operations and maintenance are maintenance technicians, vehicle console technicians, depot repair (normal wear and tear), camera overhaul, and depot repair (vandalism). (b) The cost estimate did not vary key cost driver parameters. (c) As noted above, the cost estimate did not vary key cost driver parameters. However, program officials described one sensitivity excursion that was performed in which tower quantities were varied. Specifically, the addition of one tower was shown to increase deployment costs by $2.2 million and increase operation and maintenance costs by $2.5 million (both then-year dollars).

Practice	Description	Met?	Results
(9) Was a risk and uncertainty analysis conducted?	A cost estimate is a prediction based on assumptions, constraints, and unknowns, and thus the risk exists that actual costs will differ from the estimate. To understand this risk and associated uncertainty, both should be analyzed. Specifically, (a) a probability distribution for each cost element's uncertainty should be modeled to identify risk; (b) relationships among cost elements should be assessed to capture risk; (c) a Monte Carlo simulation[d] to develop a distribution of total possible costs and derive an S curve[e] to show alternative cost estimate probabilities should be conducted; (d) a probability should be associated with the point estimate; (e) contingency reserves should be recommended for achieving the desired confidence level; (f) the risk-adjusted estimate should be developed, and the associated risks should be identified for mitigation; and (g) a plan should be implemented jointly with the contractor for identifying, analyzing, mitigating, and tracking risks.	Partially	A risk and uncertainty analysis was conducted, but it was limited. In particular: (a) Probability distributions were modeled for each cost element based on engineering judgment, rather than discrete analysis. However, since some cost elements, as noted earlier, such as those associated with government activities and development of software for the common operating picture, were excluded, the uncertainty analysis does not capture all risks. (b) Relationships among cost element estimates were assessed. However, since, as noted earlier, some cost elements were excluded, this assessment does not capture all risks. (c) A Monte Carlo simulation model that used the Latin Hypercube algorithm was conducted to derive a cumulative density function S-curve. (d) A probability was identified for the point estimate in the documentation. Specifically, the point estimate of $984.5 million (then-year dollars) is at the 37 percent confidence level, and is bounded by a low estimate of $895 million (at the 10th percentile) and a high estimate of $1,140 million (at the 90th percentile). However, the estimate does not specify a target confidence level, and it has not been updated to include risk ranges and confidence levels for the revised point estimate of $1.302 billion. (e) Program officials stated that contingency reserves were estimated, but the estimate documentation does not identify either the amount of reserves or the desired confidence level. (f) Program officials stated that a risk-adjusted budget estimate was developed. However, no documentation exists to demonstrate this. (g) The SPO has a risk management plan, and its risk database identifies seven cost-related risks that were opened in 2008. However, none of these seven risks mention the cost estimate or life cycle costs as part of the risk description.

Practice	Description	Met?	Results
(10) Was the estimate documented?	Documentation should describe the cost estimating process, data sources, and methods, so that a cost analyst unfamiliar with the program could understand how the estimate was derived. Among other things, (a) actual costs and program changes should be documented and available to update the estimate; (b) narrative and cost tables, including an executive summary, introduction, and descriptions of methods, should be used to describe the estimate. Further, data should be broken out by WBS elements, and sensitivity analysis, risk and uncertainty analysis, management approval, and updates to reflect actual costs and program changes should be documented; (c) the 12 key practices in this table should be cited or referenced; (d) contingency reserves and how they were derived from risk and uncertainty analysis should be discussed; and (e) an electronic copy of the cost estimate should exist.	Substantially	Most, but not all, aspects of the cost estimate, such as the data and calculations associated with the WBS elements, were documented in enough detail so that an analyst unfamiliar with the program could use the documentation to recreate the estimate and get the same results. Specifically: (a) Actual costs and program changes were generally not used to regularly update the estimate. (b) The document's introductory sections include a program overview, program description, program strategy, documentation overview, and program cost baseline overview. The body was organized in accordance with the WBS, thus providing a logical flow structure, and the narrative was supported by cost tables for each major section. The documentation also included some analysis of risks, but did not include a sensitivity analysis and management approval of the estimate, and it did not address how the estimate is updated to reflect actual costs and program changes. (c) The documentation does not explicitly identify the twelve practices. However, the cost estimate does address these practices to varying degrees. (d) Contingency reserves and the associated level of confidence for the risk-adjusted cost estimate are not documented. (e) An electronic version of the cost estimate exists.

Practice	Description	Met?	Results
(11) Was the estimate presented to, and approved by, management?	A briefing should be prepared for management that contains enough detail to show that the estimate is accurate, complete, and reliable, and management should approve the estimate. More specifically, (a) the briefing should include an overview of the program's technical foundation and objectives, the life cycle cost estimate in time-phased constant year dollars, a discussion of ground rules and assumptions, the method and process for each WBS cost element estimate including data sources, the results of sensitivity and risk/uncertainty analysis along with a confidence interval, the comparison of the point estimate to an independent cost estimate along with any differences, an affordability analysis based on funding and contingency reserves, a discussion of any concerns or challenges, as well as conclusions about the estimate's reasonableness and recommendations for approval, and (b) feedback from management should be acted on and documented, along with management's approval of the estimate.	Minimally	The cost estimate was briefed to the CBP Investment Review Board and was approved by management. However, the briefing was not detailed enough to show that the estimate is accurate, complete, and reliable. Specifically: (a) The briefing contains information on the approach and methods used and the estimate itself. Specifically, the briefing included a high-level overview of the program's technical foundation, the cost estimating method for each WBS cost element, and the results of risk/uncertainty analysis along with a confidence interval and a level of confidence for the point estimate, and a discussion of affordability. However, the briefing did not include the results of a sensitivity analysis, a discussion of ground rules and assumptions, the life cycle cost estimate in both time-phased constant year dollars and then-year dollars, or identify a level of contingency reserve associated with a risk-adjusted cost estimate. In addition, it did not include a comparison or reconciliation of the estimate with an independent cost estimate. (b) According to program officials, feedback was received from various parties to whom the briefing was provided, but the feedback was not documented. Among others, the briefing was provided to the SBI Executive Director, CBP Investment Review Board, the DHS Cost Analysis Division, and the DHS Acquisition Review Board on the estimate. The estimate was approved in March 2009 by the DHS Deputy Secretary as the Acquisition Authority for SBI*net*.
(12) Is the estimate updated to reflect actual costs and program changes?	The cost estimate should be updated to ensure that it is current. Specifically, (a) the estimate should be regularly updated to reflect relevant changes to the technical and program baseline; (b) the estimate should incorporate actual costs when available; and (c) the estimate should address lessons learned for elements whose actual costs differed from the estimate.	Minimally	The estimate is not routinely updated and reasons for variances between estimated and actual costs are not addressed. (a) The cost estimate documentation highlights 10 adjustments that were made to reconcile the estimate with the Acquisition Program Baseline. However, the estimate has not been updated to reflect current information on an ongoing basis. For example, the estimate does not reflect development and testing activities that were added since the estimate was approved to correct problems discovered during testing. (b) Program officials stated that they do not use actual cost data from EVM reports to update the estimate. (c) Reasons for cost variances, and thus lessons learned, are not addressed.

Source: GAO analysis of DHS data.

[a]The WBS is a document that defines in detail the work necessary to complete a program's objectives.

[b]EVM is a management tool for monitoring a program's cost and schedule performance by measuring the value of the work accomplished in a given period, compared to the planned value of work scheduled for that period and the actual cost of work accomplished.

[c]Office of Management and Budget, *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs*, Circular A-94 Revised, (Washington, D.C., Oct. 29, 1992).

[d]A Monte Carlo simulation involves the use of random numbers and probability distributions to examine outcomes.

[e]An S curve is a cumulative probability distribution, most often derived from a simulation, such as Monte Carlo, that is particularly useful in portraying the uncertainty implications of various cost estimates.

Appendix VI: 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), David Alexander, Rebecca Alvarez, Carl Barden, Tisha Derricotte, Neil Doherty, Nancy Glover, Dan Gordon, Cheryl Dottermusch, Thomas J. Johnson, Kaelin P. Kuhn, Jason T. Lee, Lee McCracken, Jamelyn Payan, Karen Richey, Karl W.D. Seifert, Matt Snyder, Sushmita Srikanth, Jennifer Stavros-Turner, Stacey L. Steele, and Karen Talley 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 afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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