United States Government Accountability Office

GAO

Report to Congressional Requesters

January 2010

SECURE BORDER INITIATIVE

DHS Needs to Address Testing and Performance Limitations That Place Key Technology Program at Risk

GAO

Accountability ★ Integrity ★ Reliability

GAO-10-158

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-10-158, a report to congressional requesters

Why GAO Did This Study

The Department of Homeland Security's (DHS) Secure Border Initiative Network (SBI*net*) is a multiyear, multibillion dollar program to deliver surveillance and decision-support technologies that create a virtual fence and situational awareness along the nation's borders with Mexico and Canada. Managed by DHS's Customs and Border Protection (CBP), SBI*net* is to strengthen CBP's ability to identify, deter, and respond to illegal breaches at and between border points of entry. Because of the program's importance, cost, and risks, GAO was asked to, among other things, determine (1) whether SBI*net* testing has been effectively managed, including the types of tests performed and whether they were well planned and executed, and (2) what the results of testing show. To do this, GAO reviewed test management documentation, including test plans, test cases, test procedures, and results relative to federal and related guidance, and interviewed program and contractor officials.

What GAO Recommends

GAO is making four recommendations to DHS related to the content, review, and approval of test planning documentation and the analysis, disclosure, and resolution of system problems. DHS agreed with three and partially agreed with one of the recommendations, and it described actions under way and planned to address them.

View GAO-10-158 or key components.
For more information, contact Randolph C. Hite, (202) 512-3439 or hiter@gao.gov.

January 2010

SECURE BORDER INITIATIVE

DHS Needs to Address Testing and Performance Limitations That Place Key Technology Program at Risk

What GAO Found

DHS has not effectively managed key aspects of SBI*net* testing. While DHS's approach appropriately consists of a series of progressively expansive developmental and operational 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, while plans for component and system testing included roles and responsibilities for personnel involved in each of ten test events that GAO reviewed, none of the plans adequately described risks and only two of the plans included quality assurance procedures for making changes to the plans during their execution. Similarly, while GAO's analysis of a random probability sample of test cases showed that a large percentage of the cases included procedures and expected outputs and behaviors, a relatively small percentage described the inputs and the test environment (e.g., facilities and personnel to be used). Moreover, even though the test cases largely included procedures, a large percentage were changed extemporaneously during execution in order to fulfill the purpose of the test. While some of the changes were minor, others were more significant, such as rewriting entire procedures and changing the mapping of requirements to cases. Further, 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 with the contractor. Compounding the number and significance of changes are questions raised by the SBI*net* program office and a support contractor about the appropriateness of some changes. For example, a program office letter to the prime contractor stated 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. Program officials attributed these weaknesses to time constraints and guidance limitations. Because of these issues, the risk that testing has not sufficiently supported objectives, exercised program requirements, and reflected the system's ability to perform as intended is increased.

From March 2008 through July 2009, about 1,300 SBI*net* defects have been found, with the number of new defects identified generally increasing faster than the number being fixed—a trend that is not indicative of a system that is maturing. Further, while the full magnitude of these unresolved defects is unclear because the majority were not assigned a priority for resolution, several of the defects that have been found have been significant. Although DHS reports that these defects have been resolved, they have caused delays, and related problems have surfaced that continue to impact the program's schedule. Further, an early user assessment raised concerns about the performance of key system components and the system's operational suitability. Program officials attributed limited prioritization of defects to a lack of defect management guidance. Given that key test events have yet to occur and will likely surface other defects, it is important for defect management to improve. If not, the likelihood of SBI*net* meeting user expectations and mission needs will be reduced.

Contents

Tables

Figures

Abbreviations

AJO-1	Ajo Border Patrol Station
C3I	command, control, communications, and intelligence
CBP	U.S. Customs and Border Protection
COMM	communications component
COP	common operating picture
CQT	component qualification testing
DHS	Department of Homeland Security
DOD	Department of Defense
DT&E	developmental test and evaluation
EOIR	Electro-Optical/Infrared
IT	information technology
IT&E	independent test and evaluation
IV&V	independent verification and validation
MSS	Mobile Surveillance Systems
NOC/SOC	Network Operations Center/Security Operations Center
OT&E	operational test and evaluation
RTU	Remote Terminal Unit
SAT	system acceptance testing
SBI*net*	Secure Border Initiative Network
S&T	Science and Technology Directorate
SBI	Secure Border Initiative
SPO	SBI*net* System Program Office
SQT	system qualification testing
TEMP	Test and Evaluation Master Plan
TUS-1	Tucson Border Patrol Station

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

January 29, 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 illegally 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 to strengthen the ability of CBP to detect, identify, classify, track, and respond to illegal breaches at and between ports of entry.[1]

In September 2008, we reported that SBI*net* was at risk because of a number of acquisition management weaknesses. Accordingly, we made a number of recommendations to address the weaknesses, which DHS largely agreed with and committed to addressing. Among these weaknesses were several associated with system testing. As we have previously reported, testing occurs throughout a system's life cycle and is essential to knowing whether the system meets defined requirements and performs as intended.[2] In light of SBI*net*'s high cost and risks, and because of the importance of effective testing to the program's success, you asked us to review SBI*net* testing. Our objectives were to determine (1) the extent to which testing has been effectively managed, including identifying the types of tests performed and whether they were well planned and executed; (2) what the results of testing show; and (3) what processes are being used to test and incorporate maturing technologies into SBI*net*.

To accomplish our objectives, we reviewed key testing documentation, including processes, test plans, test cases, execution logs, and results, as well as system requirements to be tested and the overall test management approach. We also analyzed a random probability sample of system test cases, and we interviewed program officials about test planning, execution, and management. We then compared this information to relevant guidance to identify any deviations and interviewed program officials as to the reasons for any deviations.

We conducted this performance audit from December 2008 to January 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

[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.

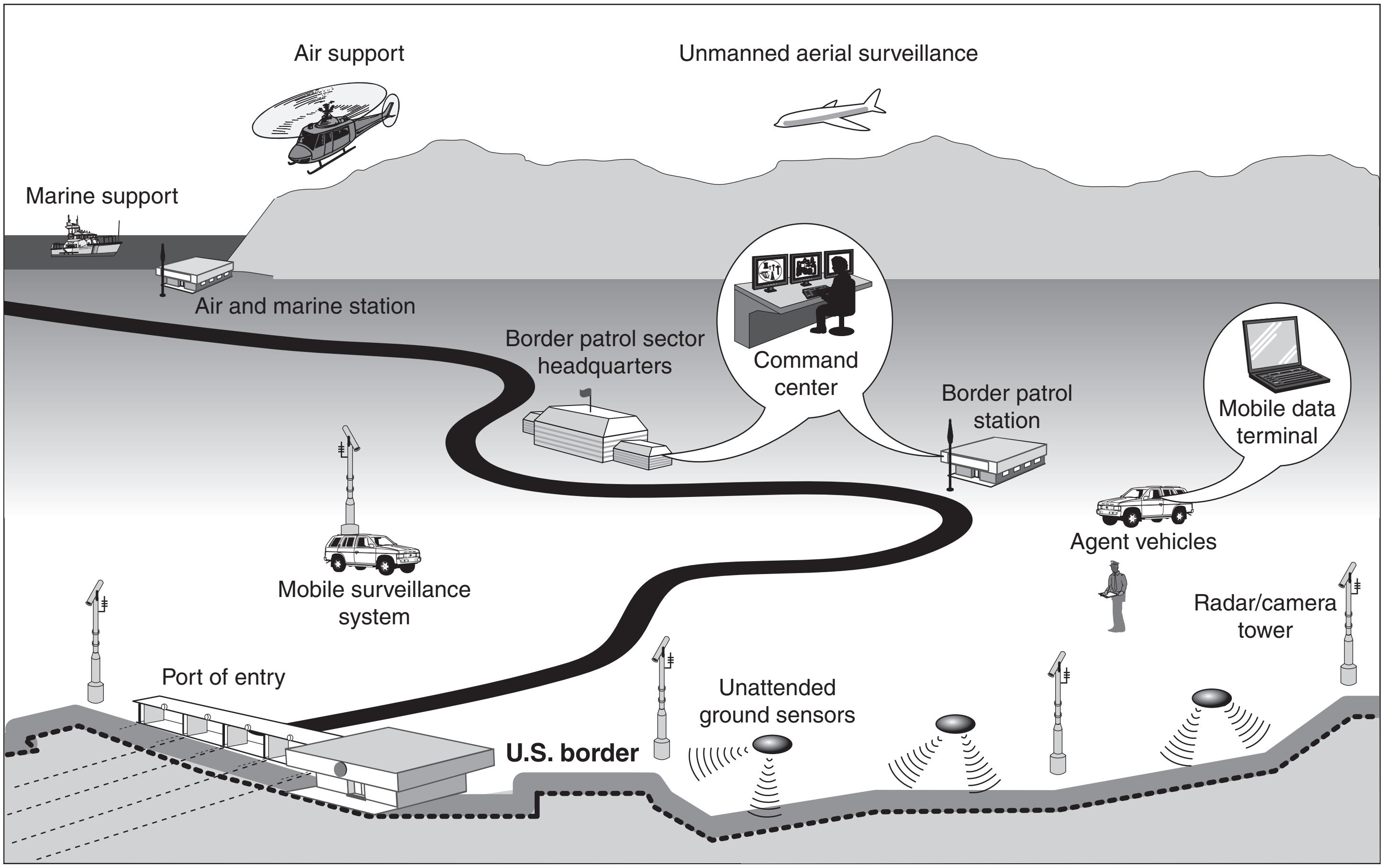
[2] See, for example, GAO, *Best Practices: A More Constructive Test Approach Is Key to Better Weapon System Outcomes*, GAO/NSIAD-00-199 (Washington, D.C.: July 31, 2000); *Office of Personnel Management: Improvements Needed to Ensure Successful Retirement Systems Modernization*, GAO-08-345 (Washington, D.C.: Jan. 31, 2008); and *Secure Border Initiative: DHS Needs to Address Significant Risks in Delivering Key Technology Investment*, GAO-08-1086 (Washington, D.C.: Sept. 22, 2008).

and conclusions based on our audit objectives. Further details of our objectives, scope, and methodology are included 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 the program has been on addressing the requirements of CBP's Office of Border Patrol, which is responsible for securing the borders between the ports of entry. Longer-term, the program is to address the 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. Figure 1 shows 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 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.

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* Acquisition Strategy

In September 2006, CBP awarded a 3-year contract to the Boeing Company for SBI*net*, with three additional 1-year options. As the prime contractor, Boeing is responsible for designing, producing, testing, deploying, and sustaining the system. In September 2009, CBP extended its contract with Boeing for the first option year.

CBP's acquisition strategy entails delivering the system incrementally in a series of discrete units of capability (blocks), in which an initial system capability is to be delivered based on a defined subset of the total requirements. Block capabilities generally include the purchase of commercially available surveillance systems, development of customized COP systems and software, and use of existing CBP communications and network capabilities. Subsequent blocks of SBI*net* capabilities are to be delivered based on feedback, unmet requirements, and the availability of new technologies. 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, thus permitting both their operational use and evaluation.

CBP's SBI Program Executive Office is responsible for managing key acquisition functions associated with SBI*net*, including tracking and overseeing the prime contractor.[3] It is organized into four areas: SBI*net* System Program Office (SPO), Systems Engineering, Business Management, and Operational Integration, and it is staffed with a mix of government personnel and contractor support staff. In addition, the SPO is leveraging other DHS resources, such as the DHS Science and Technology Directorate (S&T).

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

Recent GAO Work on SBI*net* Identified Management Weaknesses and Program Risks

In July 2008, we briefed CBP and DHS officials on the results of our then-ongoing review of SBI*net*, and in September 2008, we reported that important aspects of SBI*net* were ambiguous and in a continuous state of flux, making it unclear and uncertain what technology capabilities were to be delivered when.[4] For example, we reported that the scope and timing of planned SBI*net* deployments and capabilities had continued to change since the program began and remained unclear. Further, the SPO did not have an approved integrated master schedule to guide the execution of the program, and our assimilation of available information indicated that key milestones continued to slip. This schedule-related risk was exacerbated by the continuous change in and the absence of a clear definition of the approach used to define, develop, acquire, test, and deploy SBI*net*. Accordingly, we concluded that the absence of clarity and stability in these key aspects of SBI*net* impaired the ability of Congress to oversee the program and hold DHS accountable for results, and it hampered DHS's ability to measure the program's progress.

Furthermore, we reported that SBI*net* requirements had not been effectively defined and managed. While the SPO had issued guidance that defined key practices associated with effectively developing and managing requirements, such as eliciting user needs and ensuring that different levels of requirements and associated verification methods are properly aligned with one another, the guidance was developed after several key activities had been completed. In the absence of this guidance, the SPO had not effectively performed key requirements development 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 operational requirements, which are the basis for all lower-level requirements, were found to be unaffordable and unverifiable, thus casting doubt on the quality of the lower-level requirements that had been derived from them. As a result, we concluded that the risk of SBI*net* not meeting mission needs and performing as intended was increased, as were the chances of the system needing expensive and time-consuming rework.

We also reported that SBI*net* testing was not being effectively managed. For example, the SPO had not tested the individual system components to

[4] GAO-08-1086.

be deployed to initial locations, even though the contractor had initiated integration testing of these components with other system components and subsystems in June 2008. Further, while a test management strategy was drafted in May 2008, it 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 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 was increased, as were the chances of needed system rework.

To address these issues, we recommended that DHS assess and disclose the risks associated with its planned SBI*net* development, testing, and deployment activities; and that it address the system deployment, requirements management, and testing weaknesses that we had identified. DHS agreed with all but one of our eight recommendations and described actions completed, under way, and planned to address them. We plan to issue another report in early 2010 that, among other things, updates the status of DHS's efforts to implement our prior recommendations.

More recently, we reported that delays in deploying SBI*net* capabilities have required Border Patrol agents to rely on existing technology for securing the border that has performance shortfalls and maintenance issues.[5] For example, on the southwest border, agents rely on existing cameras mounted on towers that have intermittent problems, including signal loss.

Overview of Deployment Plans

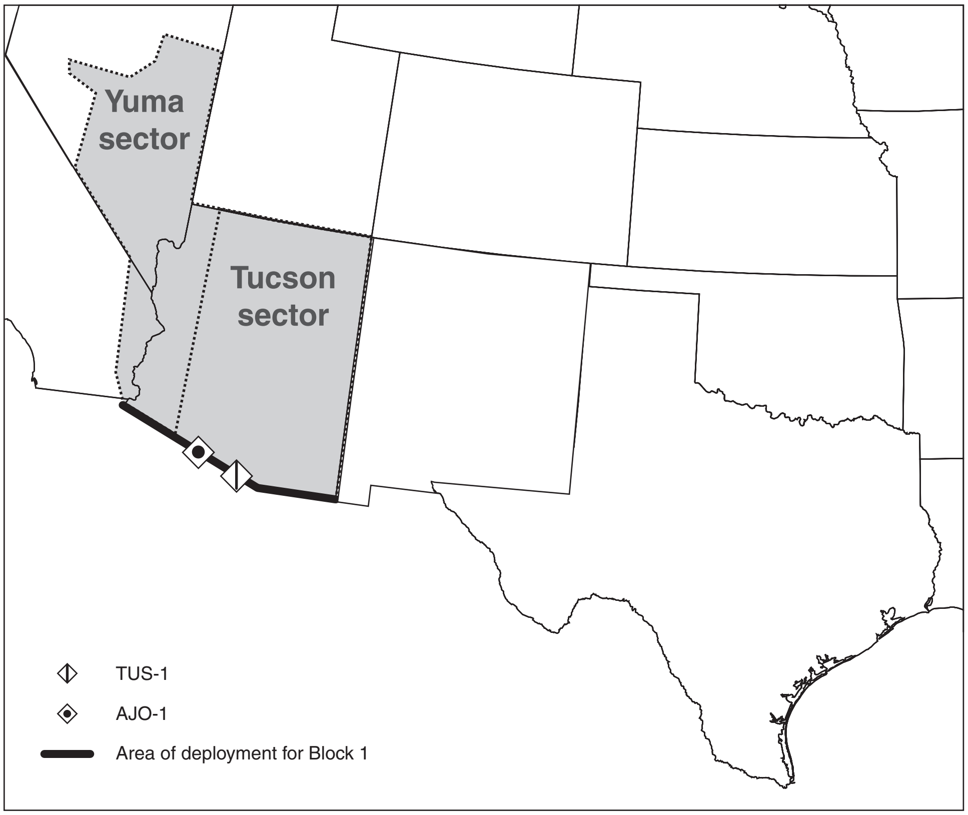
In August 2008, the DHS Acquisition Review Board[6] decided to delay the initial system deployment, known as Block 1, so that fiscal year 2008 funding could be reallocated to complete physical infrastructure projects. According to program officials, this decision also allowed more time for needed testing. In addition, the board directed the SPO to deliver a range

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

[6] The DHS Acquisition Review Board is the departmental executive board that reviews programs with life cycle costs of $300 million or more for proper management, oversight, accountability, and alignment to strategic functions of the department. The board reviews investments before approving them to proceed to the next phase of acquisition.

of program documentation, including an updated Test and Evaluation Master Plan (TEMP), detailed test plans, and a detailed schedule for deploying Block 1 to the initial two sites following completion of all integration and field testing. In February 2009, the board approved the SPO's updated documentation. A key result was a revised timeline for deploying Block 1, first to the Tucson Border Patrol Station (TUS-1), in April 2009, and then to the Ajo Border Patrol Station (AJO-1) in June 2009, both of which are located in the Tucson Sector of the Southwest border. Together, these two deployments cover 53 miles of the 1,989-mile-long southern border. Figure 2 shows the TUS-1 and AJO-1 areas of deployment.

Figure 2: TUS-1 and AJO-1 Locations Along the Southwest Border



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

The capabilities that are to be part of the Block 1 deployments at TUS-1 and AJO-1 include towers with radar and cameras mounted on them, unattended ground sensors, communications towers, and a command and control facility.

As of July 2009, the TUS-1 system was scheduled for government acceptance in February 2010. AJO-1 acceptance is to be in July 2010. Longer-term plans call for Block 1 deployments throughout the Tucson and Yuma border sectors by the summer of 2011, with additional deployments throughout the southwest border between 2011 and 2016.

DHS's Management of SBI*net* Testing Has Not Been Effective and Has Increased Program Risks

DHS has not effectively managed key aspects of the testing of SBI*net* components and the integration of these components. While DHS's testing approach appropriately consists of a series of test events, some of which have yet to be completed, plans for key events that have been performed were not defined in accordance with relevant guidance. For example, none of the plans for tests of system components addressed testing risks and mitigation strategies. Also, over 70 percent of the procedures for the key test events were rewritten extemporaneously during execution because persons conducting the tests determined that the approved procedures were not adequate. Collectively, these and other limitations have increased the risk that the deployed system will not perform as intended.

SBI*net* Testing Appropriately Consists of a Series of Developmental and Operational Test Events, but Some Have Yet to Be Completed

According to relevant leading industry practices and government guidance,[7] system testing should be progressive, meaning that it should consist of a series of test events that build upon and complement previous events in the series. These tests should 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

[7] See, for example, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Department of Defense Instruction 5000.02* (Arlington, Va., Dec. 8, 2008); Department of Homeland Security, *Acquisition Instruction/Guidebook* #102-01-001: Appendix B, Interim version 1.9 (Nov. 7, 2008); Software Engineering Institute, *Capability Maturity Model® Integration for Acquisition*, version 1.2 (Pittsburgh, Penn., November 2007); Institute of Electrical and Electronics Engineers, Inc., *Standard for Software Verification and Validation*, IEEE Std. 1012-2004 (New York, N.Y., June 8, 2005); Defense Acquisition University, *Test and Evaluation Management Guide, 5th ed.* (Fort Belvoir, Va., January 2005); and GAO, *Year 2000 Computing Crisis: A Testing Guide*, GAO/AIMD-10.1.21 (Washington, D.C.: November 1998).

the system (or major system increments) is acceptable, interoperable with related systems, and operationally suitable to users.

To its credit, the SPO has defined and is conducting a series of Block 1 tests that are progressively broader in scope and that are to verify first that individual system parts meet specified requirements, and then that these combined parts perform as intended as an integrated and operational system. These tests began with contractor-performed component characterization testing, which is informal (nongovernment witnessed) testing on the selected commercial components to verify the vendors' representation of product specifications.

According to the SBI*net* TEMP,[8] dated November 24, 2008, 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 system's engineering process and provide confidence that the system design satisfies the desired capabilities. It consists of four test events—integration testing, component qualification testing (CQT), system qualification testing (SQT), and system acceptance testing (SAT). 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. It consists of three test events—user assessment, operational test, and follow-on operational test and evaluation. (See table 1 for each test event's purpose, responsible parties, and location.)

Table 1: Overview of Key Test Events

Test events	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 and SPO witnesses	Laboratory and field test site
Component qualification testing	Verify the functional performance of individual components against component requirements.	Contractor performs and SPO witnesses	Laboratory and field test site

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

Test events	Purpose	Party responsible	Location
System qualification testing	Verify that the system design satisfies system-level requirements.	Contractor performs and 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 and SPO witnesses	Deployment site
OT&E Events			
User assessment	Identify potential operational problems and progress toward meeting desired operational effectiveness and suitability capabilities prior to deployment using the version of the system tested during system qualification testing.	Border Patrol executes in coordination with the SPO. U.S. Army Independent Test & Evaluation Team observes.	Field test site
Operational test	Determine whether the system meets defined key performance parameters in its operational environment.	Border Patrol executes with support from U.S. Army Independent Test & Evaluation Team	Deployment site
Follow-on operational test and evaluation	Evaluate changes or updates made to the system and ensure that it continues to meet operational needs.	U.S. Army Independent Test & Evaluation Team performs	Deployment site

Source: GAO analysis of DHS data.

Regression testing, which is testing to ensure that changes made to correct problems found during a test event did not introduce unintended problems, may also be performed as part of each event.

As of October 2009, the SPO reported that three of the four DT&E test events had been completed or were under way:

- Integration testing was conducted from roughly June to October 2008.
- CQT was conducted from roughly October to December 2008.[9] CQT regression testing was conducted from February to September 2009. The tested components are shown in table 2.

[9] In CBP's technical comments on a draft of this report, it characterized integration testing and CQT as being conducted in parallel and not sequentially.

Table 2: Components Tested during CQT

Name	Description
C3I COP	The hardware and software to produce a uniform picture of activities within specific areas along the border.
NOC/SOC	The Network Operations Center (NOC) and Security Operations Center (SOC) monitors networked equipment, provides alerts for network problems, protects equipment from network-based attacks, and provides user authentication.
COMM	The microwave radio communications component that transmits and receives voice, surveillance, and command and control data.
UGS	The unattended ground sensors (UGS) that detect heat and vibrations associated with foot traffic and metal associated with vehicles.
Power	The source of continuous power to the communication and sensor sites.
EOIR	The electro-optical/infrared (EOIR) tower-mounted day camera and thermal camera, which are used to help identify and classify objects.
Network	The hardware and software that transports information between system components.
Radar	The devices that track multiple objects simultaneously and provide near-real-time information on the location and movement of objects.
RTU	The devices that monitor, collect, and send health and status information from the towers and sensors to the COP or local users, and send command and control information from the COP or users to the sensors. They act as a data integration center for remote sensor data.

Source: GAO analysis of DHS data.

Note: In CBP's technical comments on a draft of this report, it stated that the Fixed Tower System was also a component tested during CQT. However, we did not receive documentation related to testing for this component, therefore it was not included as part of our analysis.

- SQT was conducted from December 2008 to January 2009. SQT regression testing is ongoing; the first round of regression testing began in February 2009, and a second round began in October 2009 and is still under way.

- The first OT&E event, the user assessment, was conducted from late March to early April 2009.

- The final DT&E test event, SAT, has not yet begun. As of October 2009, it was scheduled to start in late December of 2009 for TUS-1. The final two OT&E test events are to occur after SAT has been completed and DHS accepts the system.

Test Plans Were Not Well Defined

Effective testing includes developing well-defined test plans. According to the relevant guidance,[10] test plans should specify each of the following key elements:

- **Roles and responsibilities:** Identifies individuals or groups that are to perform each aspect of the specific test event, such as test operators and witnesses, and the functions or activities they are to perform.
- **Environment and infrastructure:** Identifies the physical facilities, hardware, software, support tools, test data, personnel, and anything else necessary to support the test event.
- **Tested items and approach:** Identifies the object of testing (such as specific software or hardware attributes or interfaces) and describes the method used to ensure each feature of these objects is tested in sufficient detail.
- **Traceability matrix:** Consists of a list of the requirements that are being tested and maps each requirement to its corresponding test case(s), and vice versa.
- **Risk and mitigation strategies:** Identifies issues that may adversely impact successful completion of testing, the potential impact of each issue, and contingency plans for mitigating or avoiding these issues.
- **Testing schedule:** Specifies milestones, duration of testing tasks, and the period of use for each testing resource (e.g., facilities, tools, and staff).
- **Quality assurance procedures:** Defines a process for ensuring the quality of testing, including steps for recording anomalies or defects that arise during testing and steps for making changes to approved procedures.

The plans for the nine CQT events and for the one SQT event were written by the prime contractor and reviewed by the SPO. These 10 plans largely satisfied four of the seven key elements described above (see fig. 3 below). Specifically, each plan included the roles and responsibilities for personnel involved in the specific test event, and most of the ten plans described the environment and infrastructure necessary for testing, explicitly identified the tested items and approach, and included traceability matrices. However, two of the plans' mappings of

[10] Institute of Electrical and Electronics Engineers, Inc., *Standard for Software and System Test Documentation*, IEEE Std. 829-2008 (New York, N.Y., July 18, 2008).

requirements to test cases contained gaps or errors. Specifically, the NOC/SOC plan mapped 28 out of 100 requirements to incorrect test cases. Further, the RTU plan did not map 6 out of 365 requirements to any test case, making it uncertain if, or how, these requirements were to be tested.

Figure 3: Extent to Which Component and System Qualification Test Plans Satisfied Relevant Guidance

	CQTs									SQT
Key elements	C3I COP	NOC/SOC	COMM	UGS	POWER	EOIR	NETWORK	RADAR	RTU	
Roles and responsibilities	●	●	●	●	●	●	●	●	●	●
Environmental and infrastructure	●	◐	●	●	●	●	●	●	●	●
Tested items and approach	●	◐	●	●	●	●	●	●	◐	●
Traceability Matrix	●	◐	●	●	◐	●	●	●	◐	●
Risk and mitigations	○	○	◐	◐	◐	◐	◐	◐	○	◐
Testing schedule	●	○	○	○	○	○	○	○	○	○
Quality assurance procedures	○	●	◐	◐	◐	◐	●	◐	◐	◐

○ Did not satisfy any aspects of the key element

◐ Satisfied some but not all aspects of the key element

● Satisfied all aspects of the key element

Source: GAO analysis of DHS data.

Further, most test plans did not fully satisfy any of the three other key elements. First, the plans did not describe any risks that would have adversely impacted the successful completion of specific tests, other than noting the safety risk to participants, even though program officials acknowledged such risks existed. For example, program officials told us that the NOC/SOC component was tested on a nonsecure laboratory network that does not resemble the environment in which it is to be fielded, which increases the risk that testing results will not accurately demonstrate the component's performance when deployed. Nonetheless, this test plan did not identify this risk and provide mitigation steps. Program officials agreed that the plans did not document testing risks, but stated that risks were generally discussed and documented during test readiness reviews, including a discussion of potential risks, and actions to mitigate them or a decision to accept them. However, our analysis of test readiness review documents for the SQT and CQT events showed that only the SQT documents discussed risk; the nine CQT documents did not.

Second, nine test plans did not include or reference a schedule for activities that showed the estimated time necessary to perform each testing task or the required period of use for testing resources. This increases the risk that resources necessary for testing may not be available when needed. According to the SBI*net* independent verification and validation (IV&V)[11] contractor, this actually was experienced. For example, the contractor reported that groups performing unrelated activities required access to the same resources needed for RTU testing, thus causing the test event to be interrupted several times because of competing demands for these resources.

Lastly, the test plans did not adequately define quality assurance procedures. For example, while nine plans described procedures for recording anomalies or defects, eight plans did not include procedures for making changes to the plan during test execution. This is important because, as discussed below, test operators made numerous changes to the procedures in every test plan that we reviewed.

Program officials told us they, too, had concerns about the quality and rigor of tests and documentation that was created by the prime contractor. Based on these concerns, they tasked the IV&V contractor with assessing the quality of the test documentation prepared by the prime contractor. Among other things, the IV&V contractor reported major deficiencies in the test plans, including requirements that had not been accurately mapped to test cases. Further, the IV&V contractor reported that certain tests did not fully exercise all requirements. For example, SQT did not include any security-related NOC/SOC requirements.[12]

These limitations in the test plans are attributable to a number of factors. Program officials told us that they did not have detailed guidelines or criteria for assessing the quality of the prime contractor's test-related deliverables, and they had insufficient time and resources to review these

[11] In 2008, the SPO contracted with an IV&V agent to, among other things, further review the program's test documentation, execution, and related processes. Generally, the purpose of IV&V is to independently ensure that program processes and products meet quality standards. The use of an IV&V function is recognized as an effective practice for large and complex system development and acquisition programs, like SBI*net*, as it provides objective insight into the program's processes and associated work products.

[12] In CBP's technical comments on a draft of this report, it stated that NOC/SOC security requirements were included in a subsequent phase of SQT testing and that testing of these requirements is also to occur as part of TUS-1 security certification and accreditation.

deliverables. Specifically, neither the TEMP nor the task orders sufficiently describe required content for test plans. Absent such guidance and resources, reviewers told us that they assessed testing documents based on their own knowledge and experiences as subject matter experts. Further, the IV&V contractor reported, and program officials confirmed, that the government waived the contractually required review period for one test plan, resulting in the SPO not reviewing the plan before the test event. Program officials told us that they also skipped other preparation activities, such as testing dry runs,[13] due to time pressure.

As discussed next, such limitations resulted in demonstrated problems during test execution. Further, they increased the risk that SBI*net* program testing was not sufficient to fully assess system performance.

Test Cases Were Not Well Defined

According to relevant guidance,[14] test cases are used to guide the execution of each test event. Among other things, well-defined test cases are to include the following:

- **Objective:** The purpose of the test case.
- **Outcomes:** The outputs and expected behaviors produced by executing the procedure, including exact values.
- **Procedure:** An ordered description of the steps that must be taken to execute each test case.
- **Environment:** The conditions needed for test setup; execution; and results recording, such as hardware and software items and their characteristics and configuration; the facilities to be used; or personnel requiring specific training.
- **Inputs:** The information required to execute each test case, such as specific input values, files, tables, or databases.

[13] Testing dry runs are conducted to ensure the test setup and procedures are mature enough to proceed into formal test events.

[14] Institute of Electrical and Electronics Engineers, Inc., IEEE Std. 829-2008.

- **Dependencies:** The sequence in which test cases need to be executed, if applicable.

Program officials told us that SQT and CQT test cases were developed by the contractor and reviewed by the SPO. Of the 12 SQT test cases, each one contained all applicable key elements. However, all 12 test cases required changes to the procedures in order to adequately exercise and verify the requirements being tested, as discussed in the next section of the report.

In contrast to the SQT test cases, the 251 CQT test cases[15] largely satisfied three of the six key elements, while less than one-half satisfied the remaining three elements (see fig. 4). We estimate that 92 percent[16] of component test cases listed the objective of the test case, and 90 percent[17] of the test cases described the specific outputs and expected behavior of the test case. In addition, an estimated 97 percent[18] of test cases included an ordered description of the procedure. However, as discussed in the next section of this report, over 70 percent of these procedures had to be revised during execution in order to fulfill the purpose of the test due to errors, omissions, or other problems.

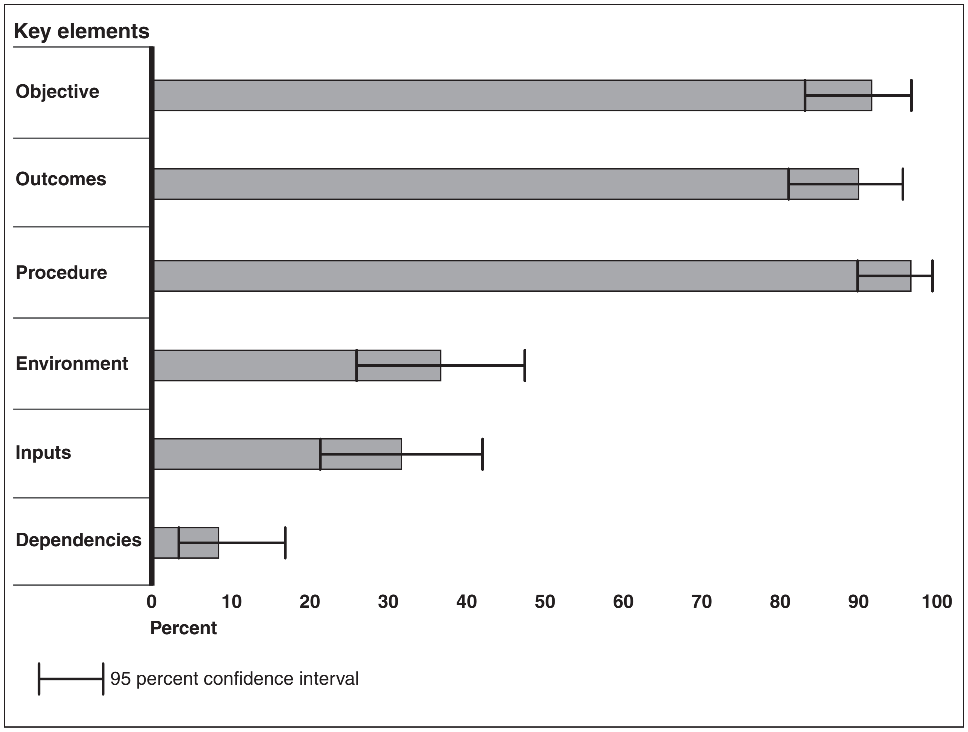
[15] We reviewed a randomly selected sample of 60 of the 251 component qualification test cases.

[16] The 95 percent confidence interval for this estimate is 83 percent to 97 percent.

[17] The 95 percent confidence interval for this estimate is 81 percent to 96 percent.

[18] The 95 percent confidence interval for this estimate is 90 percent to 99 percent.

Figure 4: Estimated Percentages of CQT Test Cases Containing Key Elements Based on a Sample of 60



Source: GAO analysis of DHS data.

Additionally, we estimate that only 37 percent[19] of CQT test cases contained a complete description of the necessary environment, including the conditions specific to the test case's execution, such as the configuration of the component(s) being tested. Without a clear description of the test environment, the risk of procedures being executed in a manner that will not fulfill the test objective is increased. In fact, the IV&V contractor identified several RTU test cases without the initial component configuration documented that failed during testing and had to be redone.

We also estimate that only 32 percent[20] of CQT test cases included the inputs required to execute the test procedures. Not documenting the

[19] The 95 percent confidence interval for this estimate is 26 percent to 47 percent.

[20] The 95 percent confidence interval for this estimate is 21 percent to 42 percent.

inputs to testing, such as specific input values, files, tables, or databases, makes it more difficult to reproduce test results, determine the root cause of related anomalies, and recreate successful test conditions.

Further, we estimate that only 8 percent[21] of CQT test cases identified other test cases upon which they were dependent. According to program officials, such dependencies may not have existed for all test cases. The IV&V contractor reported instances where the lack of clearly defined dependencies led to test cases either failing the first time and needing to be rerun, or test cases needing to be modified in order to proceed, thus resulting in unnecessary rework.

As with program test plans, SBInet officials attributed limitations in the program's test cases to a lack of detailed guidelines in the TEMP, or other criteria for assessing the quality of the prime contractor's test-related deliverables, and to having insufficient time and resources to conduct their reviews. Additionally, by skipping testing dry runs for some test events, problems that would have been found during dry runs were not identified or corrected. For example, program officials told us that a tracking system had not been tested during dry runs, and as a result, this system failed during the execution of an SQT test case, requiring the test case to be rerun. Ultimately, these limitations increase the risk of not discovering system issues during testing and not demonstrating the system's ability to perform as intended when deployed.

Testing Was Largely Not Executed According to Plans, and Changes to Plans Were Numerous, Extensive, and Not Always Appropriate

According to relevant guidance,[22] effective testing includes, among other things, executing approved test procedures as written. If necessary, this guidance states that changes to such plans should be made in accordance with documented quality assurance procedures.

In the case of SBI*net*, test procedures[23] were largely not executed as written. Further, changes to these procedures were not made according to a documented quality assurance process. Rather, they were made based on

[21] The 95 percent confidence interval for this estimate is 3 percent to 17 percent.

[22] Software Engineering Institute, *Capability Maturity Model® Integration (CMMI) for Acquisition*, version 1.2 (November 2007) and Institute of Electrical and Electronics Engineers, Inc., IEEE Std. 829-2008.

[23] As mentioned previously, test procedures are an ordered description of the steps that must be taken by each participant.

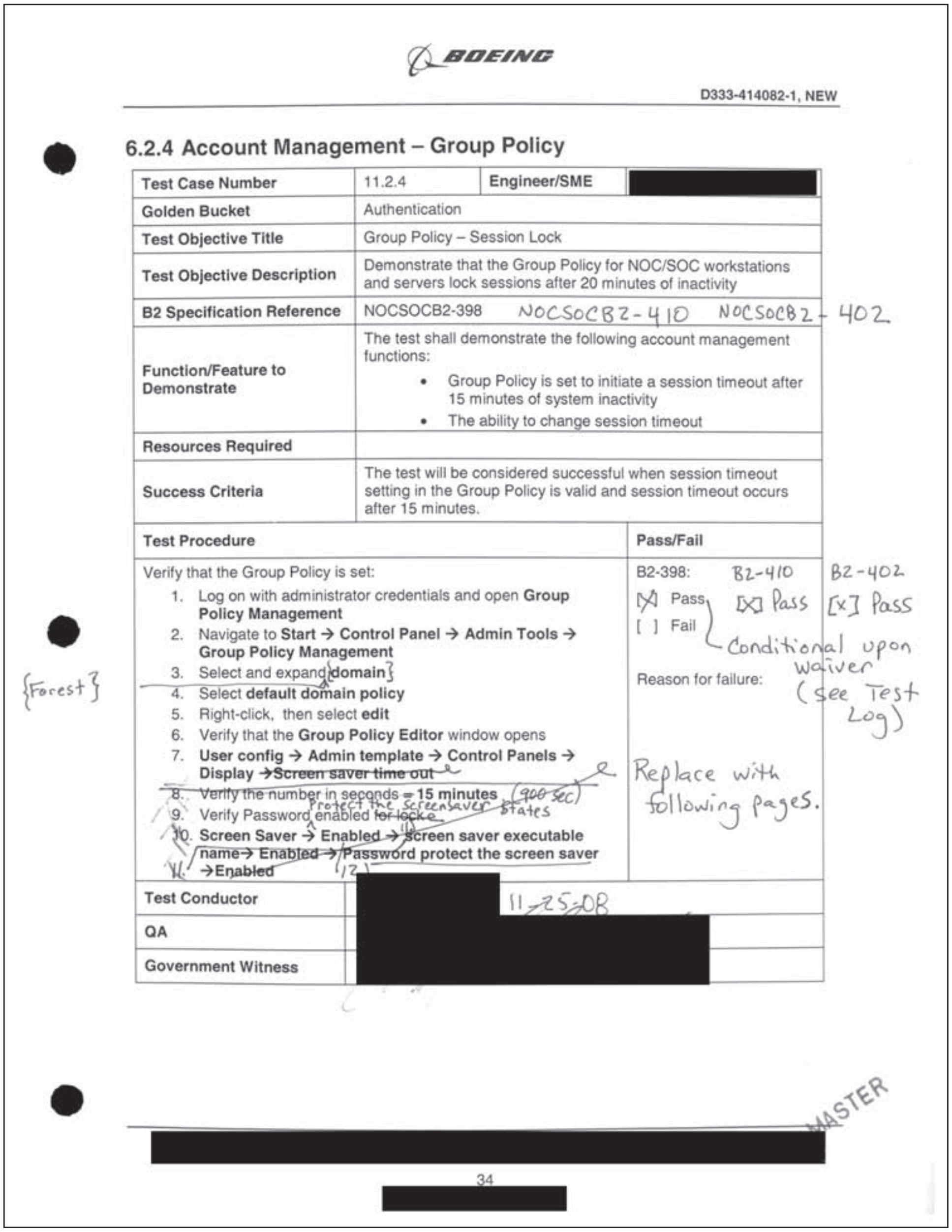
an undocumented understanding that program officials said they established with the contractor. More specifically, all 12 of the SQT test cases, as well as 211 of the 299[24] CQT test cases (a combined 72 percent) were not executed as planned. While some of these changes were relatively minor, such as changing the color of an indicator light or adding a step to "click OK" in a dialog box, others were more significant. For example, changes to the NOC/SOC or the RTU test procedures included the following:

- rewriting the entire procedure to demonstrate installation of remote software updates (RTU);
- rewriting the entire procedure to demonstrate the collection of network security logs (NOC/SOC);
- crossing out a step confirming that sensor detections had been received and handwriting that these sensors had not been tested (RTU); and
- changing the mapping of requirements to test cases (NOC/SOC).

Figure 5 on the following three pages illustrates the significant changes made to test cases using an example from the as-run log for the NOC/SOC test. As shown in the figure, test operators added requirements (as annotated in the B2 Specification Reference) and completely eliminated verification steps 8 through 11 and replaced them with 2 pages of handwritten verification steps.

[24] We stated earlier in this report that there were 263 test cases— 12 from SQT and 251 from CQT. The difference between the 299 test cases cited here and the 251 figure cited previously is due to, among other things, test cases that were executed multiple times.

Figure 5: Excerpt from NOC/SOC As-Run Log Showing Remapped Requirements and Rewritten Procedures



BOEING

D333-414082-1, NEW

6.2.4 Account Management – Group Policy

Test Case Number	11.2.4	**Engineer/SME**	[redacted]
Golden Bucket	Authentication		
Test Objective Title	Group Policy – Session Lock		
Test Objective Description	Demonstrate that the Group Policy for NOC/SOC workstations and servers lock sessions after 20 minutes of inactivity		
B2 Specification Reference	NOCSOCB2-398 NOCSOCB2-410 NOCSOCB2-402		
Function/Feature to Demonstrate	The test shall demonstrate the following account management functions: • Group Policy is set to initiate a session timeout after 15 minutes of system inactivity • The ability to change session timeout		
Resources Required			
Success Criteria	The test will be considered successful when session timeout setting in the Group Policy is valid and session timeout occurs after 15 minutes.		

Test Procedure

Verify that the Group Policy is set:

1. Log on with administrator credentials and open **Group Policy Management**
2. Navigate to **Start → Control Panel → Admin Tools → Group Policy Management**
3. Select and expand {**domain**} {Forest}
4. Select **default domain policy**
5. Right-click, then select **edit**
6. Verify that the **Group Policy Editor** window opens
7. **User config → Admin template → Control Panels → Display →~~Screen saver time out~~** e
8. ~~Verify the number in seconds = **15 minutes**~~ (900 sec)
9. Verify Password enabled ~~for locke~~ Protect the screensaver states
10. **Screen Saver → Enabled →** 11 **Screen saver executable name→ Enabled →** **Password protect the screen saver →Enabled** (12)

Pass/Fail

B2-398: ☒ Pass [ ] Fail B2-410 ☒ Pass B2-402 [x] Pass

Conditional upon waiver (see Test Log)

Reason for failure:

Replace with following pages.

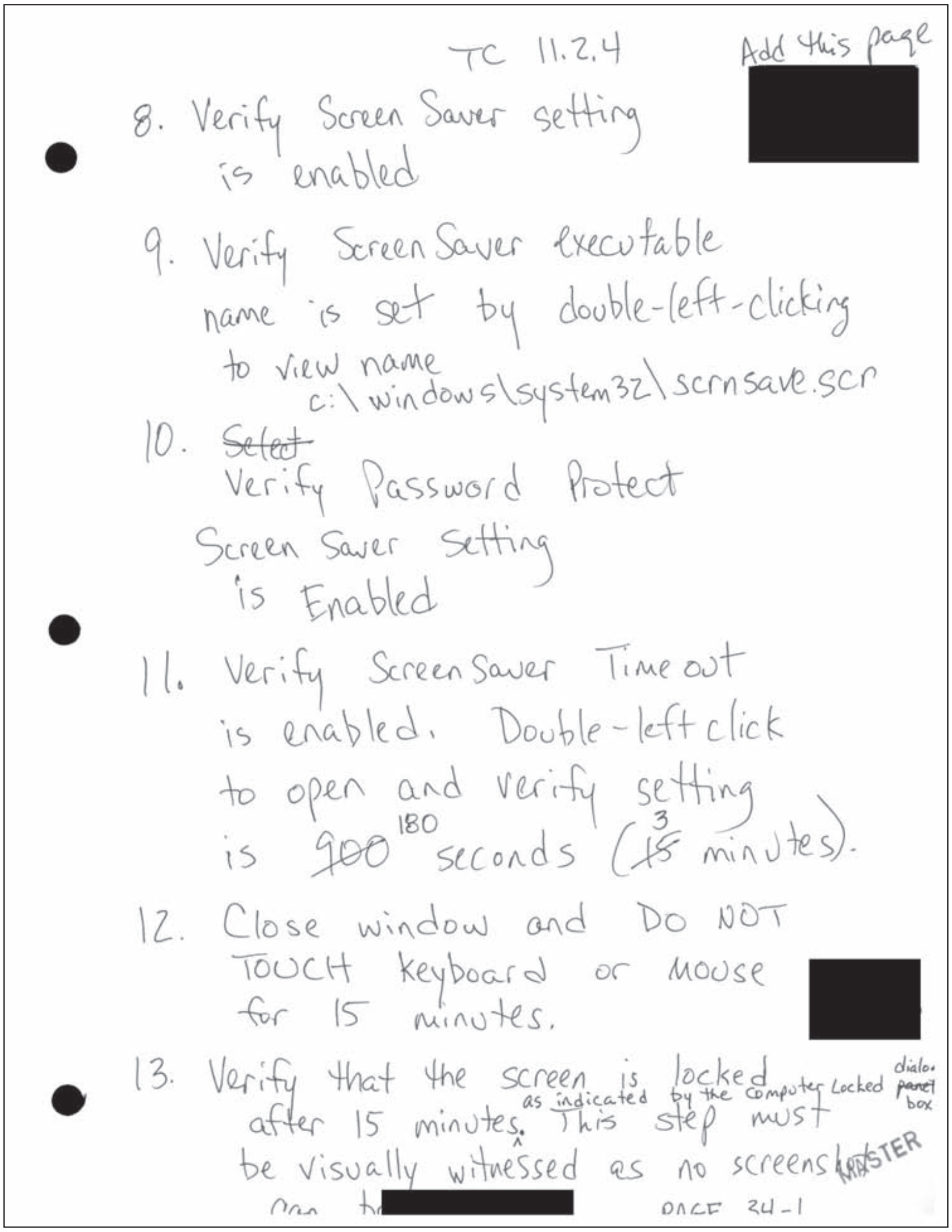
Test Conductor	[redacted] 11-25-08
QA	[redacted]
Government Witness	[redacted]

MASTER

[redacted]

34

[redacted]



TC 11.2.4 Add this page [redacted]

8. Verify Screen Saver setting is enabled

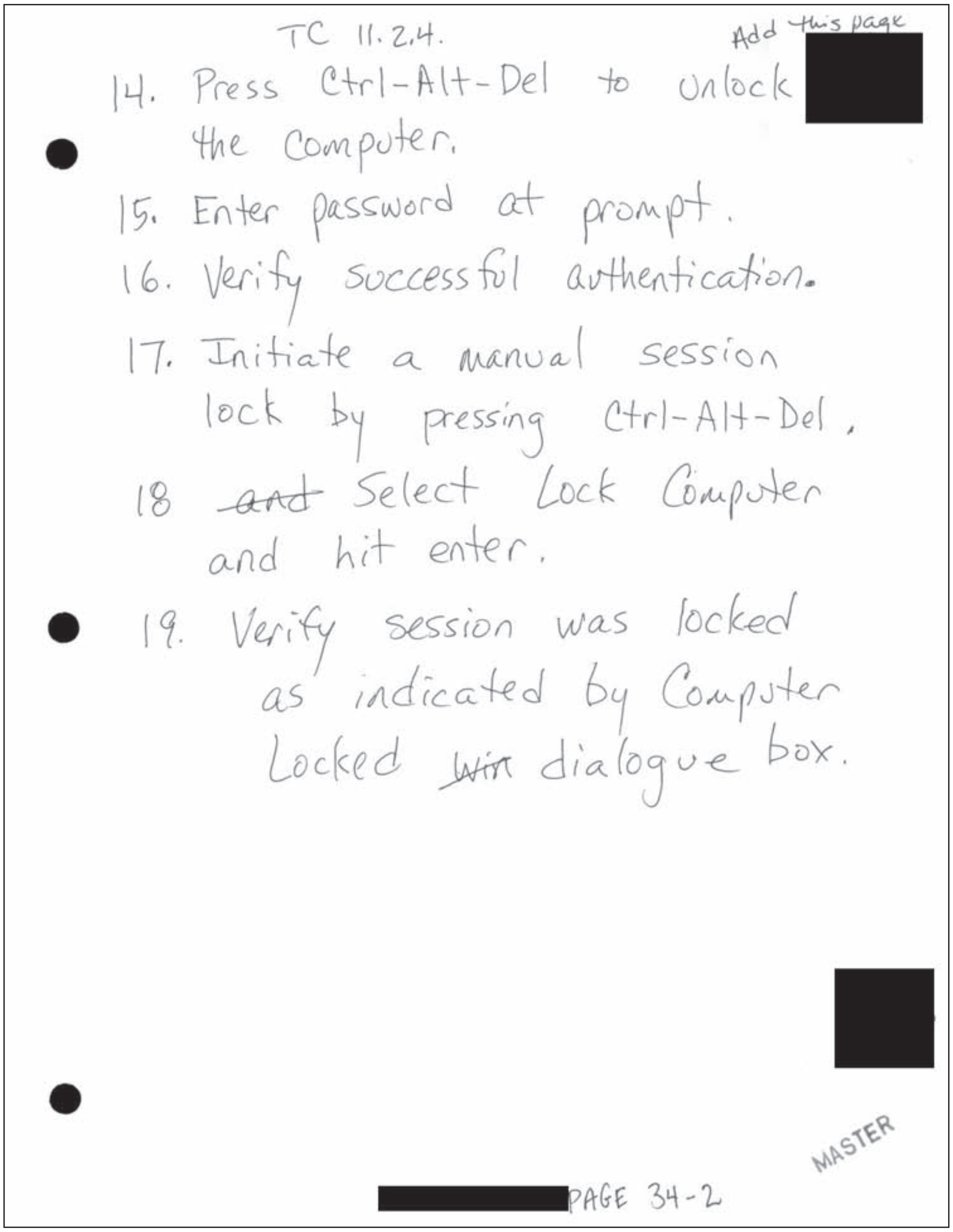
9. Verify Screen Saver executable name is set by double-left-clicking to view name c:\windows\system32\scrnsave.scr

10. ~~Select~~ Verify Password Protect Screen Saver Setting is Enabled

11. Verify Screen Saver Time out is enabled. Double-left click to open and verify setting is ~~900~~ 180 seconds (~~15~~ 3 minutes).

12. Close window and DO NOT TOUCH keyboard or MOUSE for 15 minutes. [redacted]

13. Verify that the screen is locked after 15 minutes as indicated by the Computer Locked dialo ~~panel~~ box. This step must be visually witnessed as no screensh MASTER can tr [redacted] PAGE 34-1



TC 11.2.4.

Add this page [redacted]

14. Press Ctrl-Alt-Del to unlock the computer.

15. Enter password at prompt.

16. Verify successful authentication.

17. Initiate a manual session lock by pressing Ctrl-Alt-Del.

18 ~~and~~ Select Lock Computer and hit enter.

19. Verify session was locked as indicated by Computer Locked ~~win~~ dialogue box.

[redacted]

MASTER

[redacted] PAGE 34-2

Source: DHS.

Note: Figure 5 has been redacted to, among other things, remove the names of individuals involved with SBI*net* testing activities.

These numerous and extensive changes to test cases were not made based on documented quality assurance procedures, in part, because the SPO did not establish programwide guidance describing such procedures. Instead, program officials told us that they “have an understanding” with the contractor governing how such changes are to be made.[25] According to the officials, this process allows test conductors to change the established procedures in order to make typographical corrections, insert omitted steps, or make technical adjustments as long as the contractor’s testers and quality assurance officer and the government witness approve the changes before they are executed. Based on our review of executed procedure logs, this process was generally followed.

Despite this general adherence to the process for approving test procedure changes, not all of the changes that were made and approved appear to have been appropriate, thus casting doubt on the quality of the tests and the reliability of the results. For example, in a letter to the prime contractor, dated April 2009, the SPO stated that SQT test cases required significant rework during execution, and the changes made to procedures appeared to be designed to pass the test instead of designed to qualify the system.[26] Similarly, the IV&V contractor reported instances during CQT execution where procedures had been changed in order to expedite passing the test. For example, it reported that in an RTU component test case, testers reduced the time and area scanned by radar to cover only a small, predetermined test area, ignored other areas, and passed the test case based on this reduced scope and result.

According to program officials, the numerous and extensive changes were due, in large part, to the program’s aggressive schedule—limiting the amount of time available to review and approve test cases—and the lack of testing dry runs performed. Additionally, officials stated that ambiguities in requirements caused testers to rewrite steps during execution based on interpretations of what they thought the requirements meant, which differed from that of those who wrote the original test procedures.

[25] During development testing on SBI*net*, the contractor’s staff performed the actual tests. The contractor also provided quality assurance staff and an on-site test director. Government staff served as on-site witnesses during CQT and SQT events.

[26] As stated previously, system qualification is designed to verify that the system design satisfies system-level requirements.

In CBP's technical comments on a draft of this report, it acknowledged that the changes made to test procedures were excessive, but it characterized the SQT changes as largely "procedural steps" that "did not affect the verification activity." In our view, the volume and nature of the changes made to CQT and SQT test procedures, in conjunction with the lack of a documented quality assurance process, increases the risk that the procedures did not always support test objectives, exercise program requirements, or reflect the system's ability to perform as intended. This means that system problems may not be discovered until later in the sequence of testing, such as during acceptance or operational testing.

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

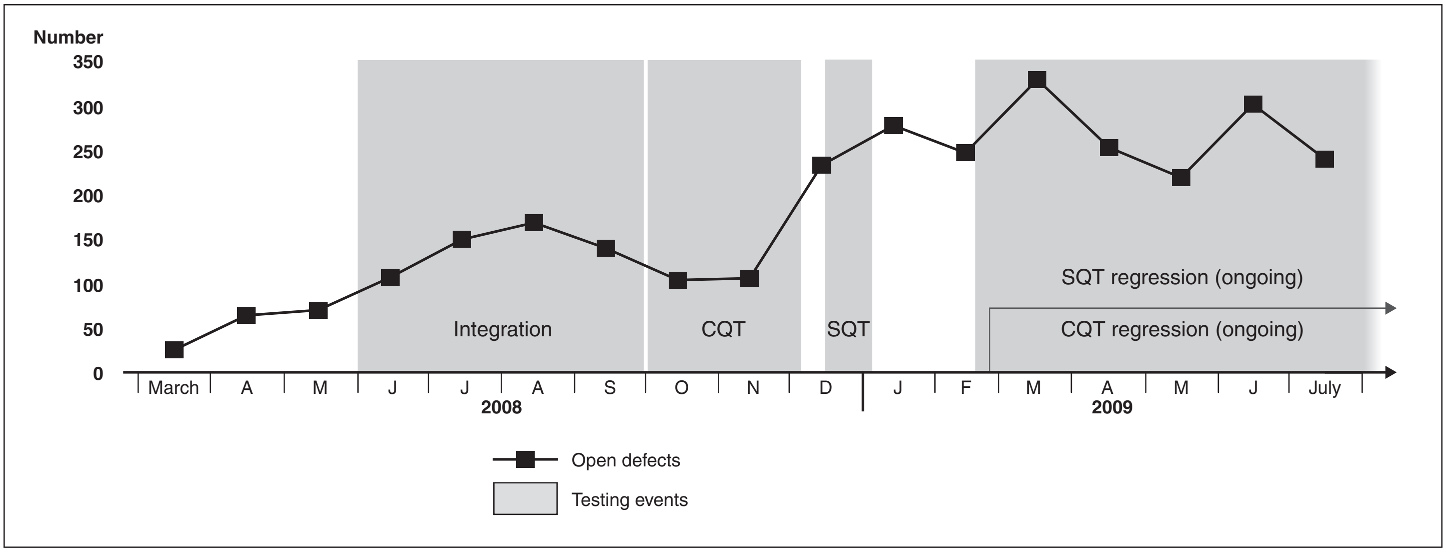
Since March 2008, the number of new SBI*net* defects has increased faster than the number of defects that have been fixed, which is not a trend that is indicative of a maturing system. In addition, weaknesses in the SPO's management of defects make their full magnitude unclear. Nevertheless, problems have already been identified that were significant enough to delay the system's schedule and necessitate system rework. Further, users recently identified concerns about the system's operational suitability.

Trends in the Number of Unresolved Defects Show That the System Is Not Maturing and Is Potentially at Risk

As previously reported,[27] testing is intended to identify and resolve system quality and performance problems as early as possible in the system life cycle. SBI*net* testing has identified a range of problems. For example, 1,333 defects were recorded from March 2008 to July 2009. During this time, the number of defects that have been resolved has generally been outpaced by the number of defects that have been identified. Figure 6 shows the trend in the number of open defects from March 2008 to July 2009.

[27] GAO, *Customs Service Modernization: Automated Commercial Environment Progressing, but Further Acquisition Management Improvements Needed*, GAO-03-406 (Washington, D.C.: Feb. 28, 2003) and *Best Practices: A More Constructive Test Approach Is Key to Better Weapon System Outcomes*, GAO-NSIAD-00-199 (Washington, D.C.: July 31, 2000).

Figure 6: Trend in the Number of Open Defects from March 2008 to July 2009



Source: GAO analysis of DHS data.

As we have previously reported,[28] such an upward trend is indicative of an immature system and can indicate a failure to meet system specifications. This is particularly problematic for SBI*net* because DHS expects final system acceptance in early February 2010.

Significant Problems Discovered during Testing Have Caused Schedule Delays and Users Have Raised Other System Concerns

Defects found during development and testing have been significant enough to delay both the deployment of Block 1 system components to TUS-1 and AJO-1 and completion of SQT. Although the SPO reports that these problems have been resolved, they have caused lengthy program delays, and other problems have surfaced that continue to impact the program's schedule. Further, an early user assessment of Block 1 operational suitability has raised additional concerns.

Among the significant defects that have been identified to date, five that surfaced during initial SQT prompted the DHS Acquisition Review Board in February 2009 to postpone the installation of sensor and communication equipment on towers at TUS-1 and to delay site preparation and installation at AJO-1 until the problems were corrected.

[28] GAO-08-345.

The five defects were: (1) the radar circuit breaker frequently tripped when the radar dish rotated beyond its intended limits, (2) COP workstations frequently crashed, (3) towers swayed beyond tolerable limits during adverse weather conditions, (4) radar clutter (i.e., false detections) occurred in adverse weather conditions, and (5) blurry camera images. As a result, sensor installation was delayed at TUS-1 by about 1 month. In May 2009, program officials reported to the Acquisition Review Board that they had either resolved or had installed operational workarounds for these five problems. Subsequently, installation resumed at TUS-1.[29]

While program officials have characterized the defects and problems found during development and testing as not being "show stoppers,"[30] they have nevertheless caused delays, extended testing, and required time and effort to fix. Moreover, the SPO and its contractor have continued to find problems that further impact the program's schedule. For example, the radar problems mentioned previously were addressed by installing a workaround that included a remote ability to reactivate the circuit breaker via software, which alleviated the need to send maintenance workers out to the tower to manually reset the circuit. However, this workaround did not fully resolve the problem, and program officials said that root cause analysis continues on related radar power spikes and unintended acceleration of the radar dish that occasionally render the system inoperable. While program officials recently told us that they believe that they have found a solution to this problem, as of October 2009, the solution was still being tested and verified. One factor that has contributed to the time and resources needed to resolve this radar problem, and potentially other problems, is the ability of the prime contractor to effectively determine root causes for defects. According to program officials, including the SBI Executive Director, the contractor's initial efforts to isolate the cause of the radar problems were flawed and inadequate. Program officials added, however, that they have seen improvements in the contractor's efforts to resolve technical issues. These radar problems have already caused SQT regression delays of about 4 months.

[29] Installation at AJO-1 was expected to begin in late 2009.

[30] David Aguilar, Chief of the U.S. Border Patrol, testified to the extent of problems found during testing to the House of Representatives Committee on Homeland Security, Subcommittee on Border, Maritime, and Global Counterterrorism on September 17, 2009.

Further, Border Patrol operators have identified a number of concerns with SBI*net* during an early user assessment. Specifically, from March 27 to April 3, 2009, CBP conducted a user assessment to give Border Patrol operators a chance to interact with Block 1 functionality and offer feedback based on their experiences. During the assessment, Border Patrol operators compared the performance capabilities of existing technology—Project 28[31] and Mobile Surveillance Systems (MSS)[32]—to those of Block 1. The user assessment took place in a field test environment. According to the assessment report, dated July 1, 2009, weather conditions during the assessment were described as "favorable," including typical wind conditions, yet the report describes a number of less than optimal results. For example, while Border Patrol operators noted that Block 1 offered functionality above what Project 28 radar offers, this functionality was not adequate for optimal operational effectiveness when detecting items of interest. Moreover, users raised concerns about the accuracy of Block 1's radar, and they characterized the range of Block 1 cameras as being operationally insufficient. Specifically, Block 1 cameras were assessed as having one-half the range of MSS's cameras, and significantly less range than the Project 28 cameras. Further, Block 1's video quality was assessed as being inconsistent. Regarding the COP, operators considered Block 1's capabilities to be a significant improvement over both the Project 28 and MSS. However, they also raised concerns about the COP's accuracy and the need for a number of relatively "small, but critical enhancements."

Program officials stated that some of the problems identified by users were attributable, in part, to the users' insufficient familiarity with Block 1. However, Border Patrol officials reported that the agents who participated in the assessment had experience with the MSS and/or Project 28 and that the agents received 2 days of training prior to the assessment. As a result, the Border Patrol reported that the issues and concerns generated should be considered operationally relevant.

[31] The first SBI*net* capabilities were deployed under a pilot or prototype effort known as Project 28.

[32] The Mobile Surveillance Systems are the current technology systems used to supplement fixed surveillance assets (such as towers and cameras) to help detect, classify, and track items of interest along the border.

System Defects Not Being Prioritized and Thus Full Magnitude of Program Risks Is Not Clear

As we have previously reported,[33] having complete and accurate defect information is necessary to adequately understand system maturity and to make informed decisions about how to best allocate limited resources to meet competing demands for resolving them. According to relevant guidance,[34] effective defect management includes having a defined process that, among other things, assigns priority to each defect and ensures that the more severe defects are given priority attention.

The SPO does not have a documented approach for prioritizing and managing the disposition of defects. Instead, program officials stated that they rely on the prime contractor to do so. However, under this approach, system defects have not been consistently assigned priorities, and in fact, a majority of them have not been prioritized. Specifically, when unplanned anomalies occur during development or testing, they are documented in contractor databases and classified as development incidents, test incidents, or “nonconformances.”[35] The anomalies or defects are then reviewed to determine if they are related to hardware or software problems or if they are deviations from engineering or design specifications and managed separately. Of the three types of defects—hardware, software, and nonconformances—only software defects are regularly assigned a priority. Each software defect’s priority is assessed on a scale of 1 to 5. In general, category 1 and 2 software defects are those that impact the system’s operation and thus must be resolved prior to beginning a subsequent test event and are likely to affect system testing. Categories 3 through 5 software defects are those that have an available workaround or have very little or no impact on system performance or testing. Although hardware incidents and nonconformances are not assigned a priority under this approach, program officials referred to

[33] GAO-08-345.

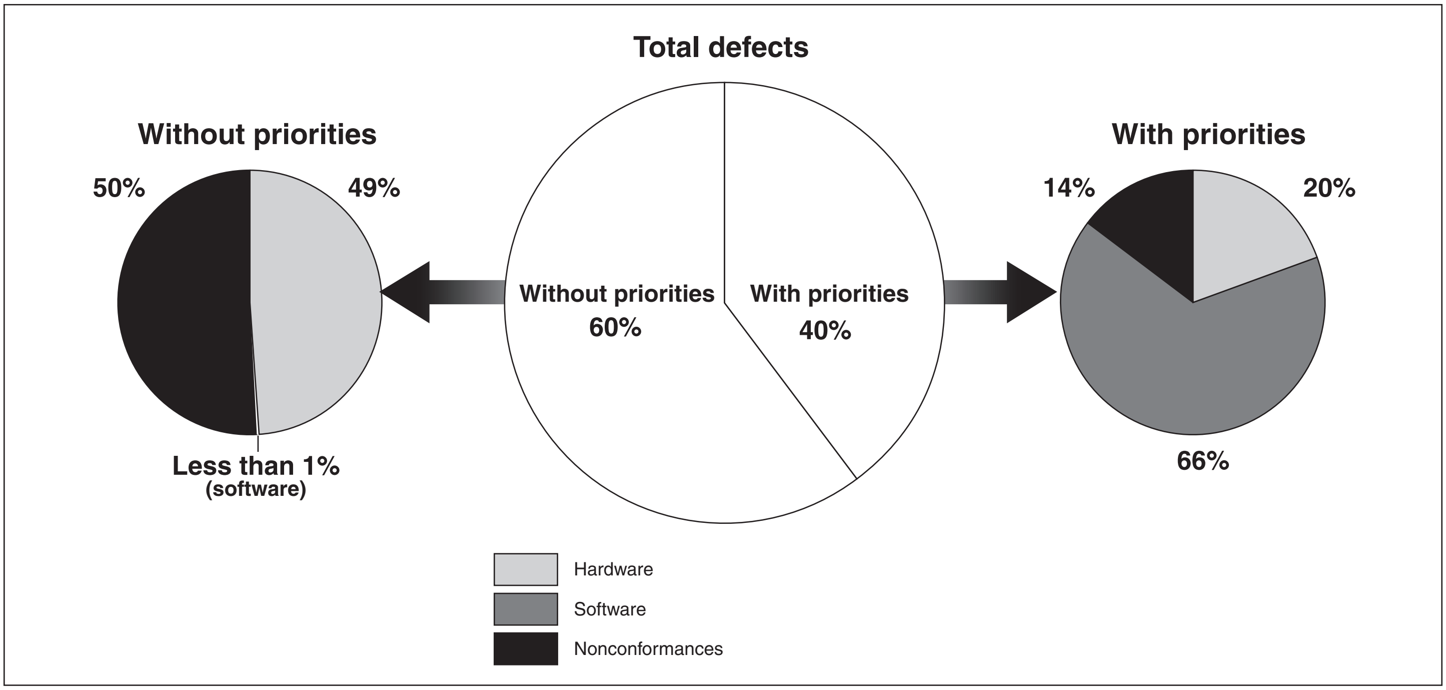
[34] DHS, *Acquisition Instruction/Guidebook* #102-01-001: Appendix B, Interim version 1.9, (November 7, 2008) and Institute of Electrical and Electronics Engineers, Inc., IEEE Std. 829-2008.

[35] According to contractor documentation, a development incident is a system incident (software), test equipment issue (hardware), requirement failure, or engineering unit failure identified during system development or informal (nongovernment witnessed) testing; a test incident is a system incident, hardware or software problem, test equipment issue, or requirement failure identified during formal testing; and nonconformances, which can be identified at any time, are problems with the reliability or quality of system hardware or software components, or any other issues that cause the system or component to not meet engineering or design specifications.

nonconformances as "must-fixes" because the contractor must address deviations from the way the system was designed.

As a result of this approach, about 60 percent (or 801 of 1,333) of Block 1 defects identified from March 2008 to July 2009 were not assigned a priority (see fig. 7). Further, contrary to the program's stated approach of not assigning priorities to hardware and nonconformances, 104 hardware defects and 77 nonconformances were assigned priorities.

Figure 7: Percentage of SBI*net* Defects with and without Assigned Priorities



Source: GAO analysis of DHS data.

The lack of defect prioritization is partially attributable to the fact that the SPO has not defined a process governing how defects are to be prioritized and managed. Officials acknowledged this and stated that they intend to have the contractor prioritize all defects in advance of future test readiness reviews. They added that they will use these reviews to ensure all priority 1 and 2 defects associated with a given test event are corrected prior to beginning the event.

Until system defects are managed on a priority basis, the SPO cannot fully understand Block 1's maturity or its exposure to related risks, nor can it make informed decisions about how best to allocate limited resources to address existing and future system defects.

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

The SPO does not have its own process for testing SBI*net*-relevant technologies that are maturing or otherwise available from industry or other government entities, including the Department of Defense (DOD). Instead, the SPO relies on DHS's Science and Technology Directorate (S&T), whose mission is to provide technology solutions that assist DHS programs in achieving their missions.[36] To accomplish its mission, S&T relies on an undocumented process. According to the S&T sensors and surveillance program manager, the following process is followed: S&T first interacts with its customers to develop system component thresholds, requirements, and metrics (e.g., the maximum false alarm rates or minimum range that a technology must have to be useful). Based on this information, the program manager said that S&T then develops a test plan and performs initial laboratory testing in conjunction with the source of the potential technology. If successful, testing is moved to an environment configured to replicate the given program's target operational environment. The final step in the process, as explained by the S&T program manager, is to perform a field-based operational evaluation in which users evaluate the technology. The program manager stated that if operational evaluation is successful, the technology is typically judged to be sufficiently mature to transition to the program office to incorporate into the system solution.

To leverage S&T, CBP signed a multiyear Interagency Agreement with the directorate in August 2007. According to this agreement, S&T is to, among other things, research, develop, assess, test, and report on available and emerging technologies that could be incorporated into the SBI*net* system solution. S&T has, to date, focused its efforts on potential technologies to fill known performance gaps or to improve upon technology choices that were already made. One area of focus has been gaps in the radar system's

[36] The SPO originally relied on its prime contractor to leverage such technologies. According to the program management task order, which was executed in April 2008, the prime contractor was to (1) collaborate with CBP and the SPO to develop an SBI*net* technology road map; (2) assess system architecture capabilities and recommend future technological enhancements; (3) identify evolving system requirements, gaps in capabilities, and potential solutions; and (4) identify new commercial products for program use. Program officials stated that this task order was modified, in part, to eliminate funding for these activities in order to focus the contractor on current development and deployment issues.

ability to distinguish true radar hits, such as a person crossing the border, from false alarms, such as those caused by clutter[37] during adverse weather conditions. In this regard, S&T reports that it has worked with industry to research and assess technology techniques for reducing clutter, as well as technology to help pinpoint the location of an item of interest along the border (e.g., laser illuminators). According to program officials, S&T is working with a contractor to develop enhanced imagery techniques to address camera performance gaps that testing found to occur during adverse weather conditions.

When researching and assessing emerging or available border security technologies, S&T officials told us that they interact with DOD components and research entities, such as the Army's Night Vision and Electronic Sensors Directorate,[38] the Institute for Defense Analysis,[39] and the Massachusetts Institute of Technology's Lincoln Laboratory. However, these officials stated that defense-related technologies are not always a good fit with SBI*net* because DOD operations are very different from those of DHS. For instance, they stated that DHS systems are designed for fixed, permanent locations, and thus need to have a long life span with minimal maintenance. Conversely, according to S&T, DOD systems are designed for short-term, changing missions and thus need to be adaptable, and disposable. Additionally, the S&T program manager told us that adapting some DOD sensor technology for DHS use can be constrained by the fact that this equipment can be classified, and some Border Patrol agents do not have the necessary security clearance to use it.

In addition, program officials told us that they too interact with several DOD components and research entities, including the Army's Night Vision and Electronic Sensors Directorate. As a result of the combined efforts of S&T and the SPO, these officials told us that the current SBI*net* system solution leverages some technologies that are used in DOD systems. For example, they said that the COP software was based on a software

[37] Clutter refers to items such as blowing trees, weather, or general interference, which radar or cameras may interpret as items of interest.

[38] The Night Vision and Electronic Sensors Directorate is the Army's research and development laboratory for night vision and other advanced sensor technologies.

[39] The Institute for Defense Analysis is a nonprofit corporation that administers three federally funded research and development centers to provide objective analyses of national security issues.

product developed by DOD, and DOD uses the same radar system as SBI*net*.

Conclusions

Effective testing is integral to successfully acquiring and deploying a large-scale, complex system of system components, like SBI*net*. As such, it is important that testing of SBI*net* components and their integration be managed with the rigor and discipline embodied in relevant guidance. To do less unnecessarily increases the risk of problems going undetected until late in the system's life cycle, such as when it is being accepted for use, or even worse, after it becomes operational. When this happens, the result is either incurring expensive and time-consuming rework to bring the system's capabilities and performance up to the point that it meets user expectations, or accepting and using a system that cannot adequately support mission operations.

SBI*net* testing has not been managed in a manner to adequately ensure that Block 1 will perform as intended. While aspects of SBI*net* test management were positive—such as its provision for testing system components and subsystems first, followed by a series of test events aimed at their integration and the overall system's ability to function as intended in settings that are increasingly more representative of the target operational environment—other aspects of test management were not. These test planning, execution, and recording weaknesses can, in large part, be attributed to a lack of guidance in the program's Test Evaluation Master Plan for assessing test documentation, including test plans and test cases, and sufficient time for reviewing and approving test documentation. Collectively, they have increased the risk that promised system capabilities and performance parameters have not been sufficiently tested to the point of providing reasonable assurance that the system will perform as intended prior to its acceptance and operational use.

This risk is compounded by the trend in the number of unresolved system problems that the test events performed to date have identified. Moreover, the full magnitude of the existing inventory of system problems is not clear because the Test and Evaluation Master Plan does not include clear and sufficient guidance, and contractor direction has not required that all problems be categorized by severity, thus precluding adoption of a truly prioritized and risk-based approach to resolving them. Given that the number of unresolved problems is well into the hundreds, and that problems that have been identified have contributed to lengthy program delays, a full understanding of the relative significance of all problems is critical to DHS's efforts to successfully deliver SBI*ne*t.

Furthermore, the chances of identifying additional problems, and thus requiring extra time and effort to resolve them, are high because key events, such as system acceptance testing and operational test and evaluation, have yet to occur. It is thus vital for DHS to immediately strengthen its management of SBI*net* testing to include defect tracking and resolution. If it does not, further program delays can be expected, and the likelihood of Block 1 meeting user expectations and mission needs will be reduced.

Recommendations for Executive Action

To improve DHS's management of SBI*net* testing, including the risk-based resolution of current and to-be-detected system problems, we recommend that the Secretary of Homeland Security direct the Commissioner of the U.S. Customs and Border Protection to have the SBI Executive Director, in collaboration with the SBI*net* Program Director, take the following four actions:

- Revise the SBI*net* Test and Evaluation Master Plan to include (1) explicit criteria for assessing the quality of test documentation, including test plans and test cases, and (2) a process for analyzing, prioritizing, and resolving program defects.
- Ensure that test schedules, plans, cases, and procedures are adequately reviewed and approved consistent with the revised Test and Evaluation Master Plan.
- Ensure that sufficient time is provided for reviewing and approving test documentation prior to beginning a given test event.
- Triage the full inventory of unresolved system problems, including identified user concerns, and periodically report the status of the highest priority defects to Customs and Border Protection and Department of Homeland Security leadership.

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 our report is factually sound, and it acknowledged the management and system engineering challenges discussed in the report. Further, the department agreed with our last three recommendations and partially agreed with the first recommendation. In this regard, it described actions under way and planned to address them and provided milestones for doing so. In addition, it referenced technical comments that were separately provided, which we have incorporated in the report, as appropriate.

Regarding its partial agreement with our first recommendation, DHS agreed that program documentation should include the information that we recommended, but did not agree that this information should be included in the Test and Evaluation Master Plan. Instead, the department stated that it plans to include the information in other program documents, such as the System Engineering Plan, Quality Management Plan, Configuration Management Plan, and detailed test plans. We support the department's decision to include this important information in key program documentation, and believe that its plans to do so are consistent with the intent of our recommendation. However, we would add that it is important that the Test and Evaluation Master Plan, which is intended to describe the overall test and evaluation approach, at least reference the documents that include the recommended information.

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 Office of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix III.

Randolph C. Hite

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

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine (1) the extent to which testing has been effectively managed, including identifying the types of tests performed and whether they were well planned and executed; (2) what the results of testing show; and (3) what processes are being used to test and incorporate maturing technologies into SBI*net*.

To identify the types of tests performed, we reviewed the program's overall test management approach as described in relevant documentation, such as the SBI*net* Test and Evaluation Master Plan dated November 2008; program management review documentation; component and system qualification test readiness reviews; and contract task orders. We also interviewed key program officials, including the Secure Border Initiative (SBI) Executive Director, the SBI*net* Program Director, the SBI*net* Director of Architecture and System Design, the SBI*net* Test Lead, and the SBI*net* Director of Business Operations.

To determine if SBI*net* tests were well planned, we focused on the test events associated with the two types of testing that had recently been completed or were under way—the nine component qualification test events and the system qualification test event. For these events, we reviewed relevant documentation, such as test plans and test cases, and we compared them to relevant guidance. More specifically, we compared the plan for each of the 10 test events against key elements described in Institute of Electrical and Electronics Engineers test documentation guidance. We also reviewed a randomly selected sample of 60 test cases from a universe of 251 component qualification test cases, and we reviewed all 12 of the system qualification test cases (a total of 263). In doing so, we compared these test cases to six key aspects of well-defined test cases, as specified in relevant guidance. We used statistical methods appropriate for audit compliance testing to estimate 95 percent confidence intervals for the test cases in our sample. 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.

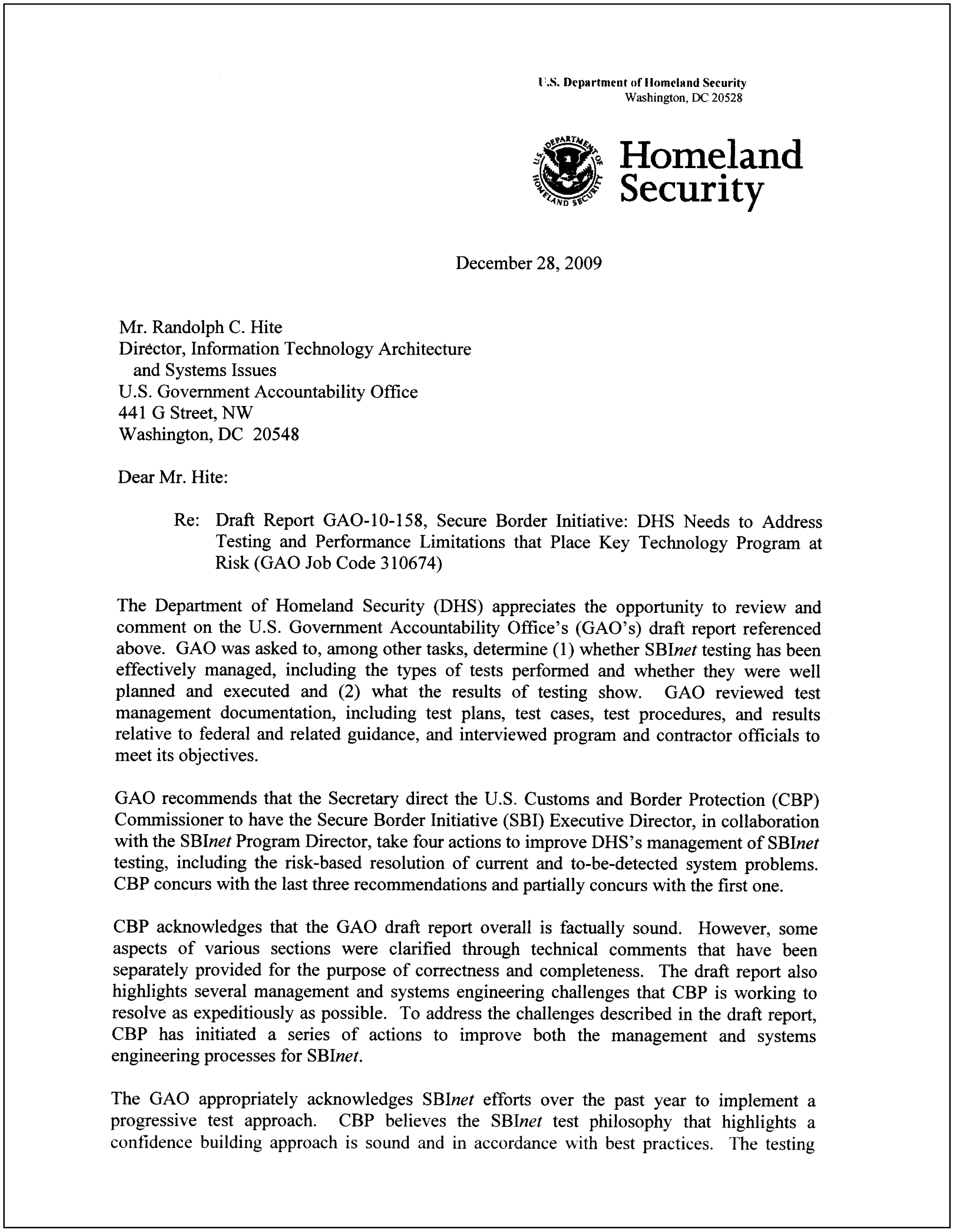
To determine if SBI*net* tests were well executed, we reviewed each of the 299 as-run procedures that had been executed as part of component qualification testing (CQT) plus the 13 that were executed as part of system qualification testing (SQT) to determine how many included changes made by test conductors to the printed procedures, and whether these changes had been approved by the contractor's quality assurance officer. This number differs from the number of planned test cases we reviewed (263) because some test cases had been added or deleted and some were executed multiple times. In addition, we interviewed program officials and prime contractor representatives to better understand the scope and content of the test cases and reasons for any deviations. We also interviewed officials from the independent verification and validation contractor and reviewed related reports to determine their role in test planning and execution. Further, we visited the prime contractor's site in Huntsville, Alabama, to interview program and contractor officials to understand how system requirements related to test cases and procedures.

To determine what the results of SBI*net* testing show, we reviewed relevant documentation, such as component and system qualification test reports, program management reviews, program office briefings, and Department of Homeland Security (DHS) Acquisition Review Board decision memoranda. We also reviewed and analyzed program data about open (i.e., unresolved) system problems (i.e., hardware and software defects and nonconformances) for the 17-month period beginning on March 2008 and ending July 2009 to determine the trend in the number of problems. Further, we analyzed the program's approach to managing these defects, including how they were prioritized for resolution. In addition, for those problems that were reported to the DHS Acquisition Review Board as significant, we analyzed the nature of the defects and tracked steps taken to address them and the extent to which these and other problems affected the program's schedule. We also interviewed program officials and prime contractor representatives to better understand the scope and nature of the selected problems and their impacts on system performance and program progress. To assess the reliability of the defect data that we used, we reviewed quality and access controls over the automated tools used to manage defect data (i.e., TipQA and ClearQuest). We determined that the data were sufficiently reliable for the purposes of this report.

To determine the process used to test and incorporate maturing technologies into SBI*net*, we reviewed relevant SBI*net* documentation, such as a contract task order, the fiscal year 2009 SBI Expenditure Plan, and the Interagency Agreement between the program office and DHS's Science and Technology Directorate (S&T). In addition, we reviewed documentation provided by the directorate related to SBI*net* and border surveillance technologies, such as technical reviews of cameras conducted by the U.S. Army's Night Vision and Electronic Sensors Directorate and S&T briefings on border technology. We also interviewed directorate and program officials to better understand the processes being followed, and to identify examples of where technologies used by the Department of Defense had been incorporated into SBI*net*.

We performed our work at the U.S. Customs and Border Protection headquarters, DHS Science and Technology Directorate, and prime contractor facilities in the Washington, D.C., metropolitan area and at a prime contractor facility in Huntsville, Ala. We conducted this performance audit from December 2008 to January 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

December 28, 2009

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:

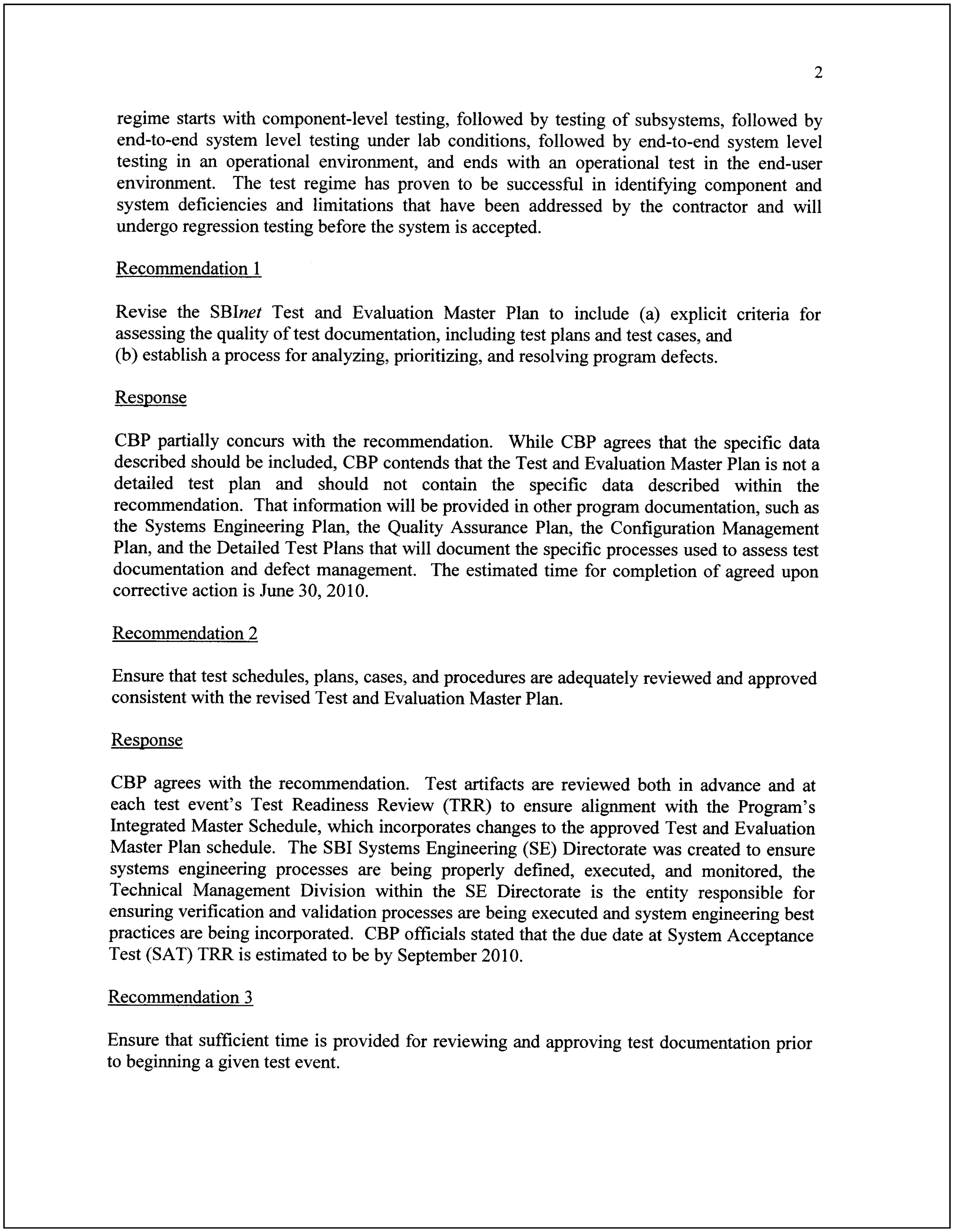
Re: Draft Report GAO-10-158, Secure Border Initiative: DHS Needs to Address Testing and Performance Limitations that Place Key Technology Program at Risk (GAO Job Code 310674)

The Department of Homeland Security (DHS) appreciates the opportunity to review and comment on the U.S. Government Accountability Office's (GAO's) draft report referenced above. GAO was asked to, among other tasks, determine (1) whether SBI*net* testing has been effectively managed, including the types of tests performed and whether they were well planned and executed and (2) what the results of testing show. GAO reviewed test management documentation, including test plans, test cases, test procedures, and results relative to federal and related guidance, and interviewed program and contractor officials to meet its objectives.

GAO recommends that the Secretary direct the U.S. Customs and Border Protection (CBP) Commissioner to have the Secure Border Initiative (SBI) Executive Director, in collaboration with the SBI*net* Program Director, take four actions to improve DHS's management of SBI*net* testing, including the risk-based resolution of current and to-be-detected system problems. CBP concurs with the last three recommendations and partially concurs with the first one.

CBP acknowledges that the GAO draft report overall is factually sound. However, some aspects of various sections were clarified through technical comments that have been separately provided for the purpose of correctness and completeness. The draft report also highlights several management and systems engineering challenges that CBP is working to resolve as expeditiously as possible. To address the challenges described in the draft report, CBP has initiated a series of actions to improve both the management and systems engineering processes for SBI*net*.

The GAO appropriately acknowledges SBI*net* efforts over the past year to implement a progressive test approach. CBP believes the SBI*net* test philosophy that highlights a confidence building approach is sound and in accordance with best practices. The testing



regime starts with component-level testing, followed by testing of subsystems, followed by end-to-end system level testing under lab conditions, followed by end-to-end system level testing in an operational environment, and ends with an operational test in the end-user environment. The test regime has proven to be successful in identifying component and system deficiencies and limitations that have been addressed by the contractor and will undergo regression testing before the system is accepted.

Recommendation 1

Revise the SBI*net* Test and Evaluation Master Plan to include (a) explicit criteria for assessing the quality of test documentation, including test plans and test cases, and (b) establish a process for analyzing, prioritizing, and resolving program defects.

Response

CBP partially concurs with the recommendation. While CBP agrees that the specific data described should be included, CBP contends that the Test and Evaluation Master Plan is not a detailed test plan and should not contain the specific data described within the recommendation. That information will be provided in other program documentation, such as the Systems Engineering Plan, the Quality Assurance Plan, the Configuration Management Plan, and the Detailed Test Plans that will document the specific processes used to assess test documentation and defect management. The estimated time for completion of agreed upon corrective action is June 30, 2010.

Recommendation 2

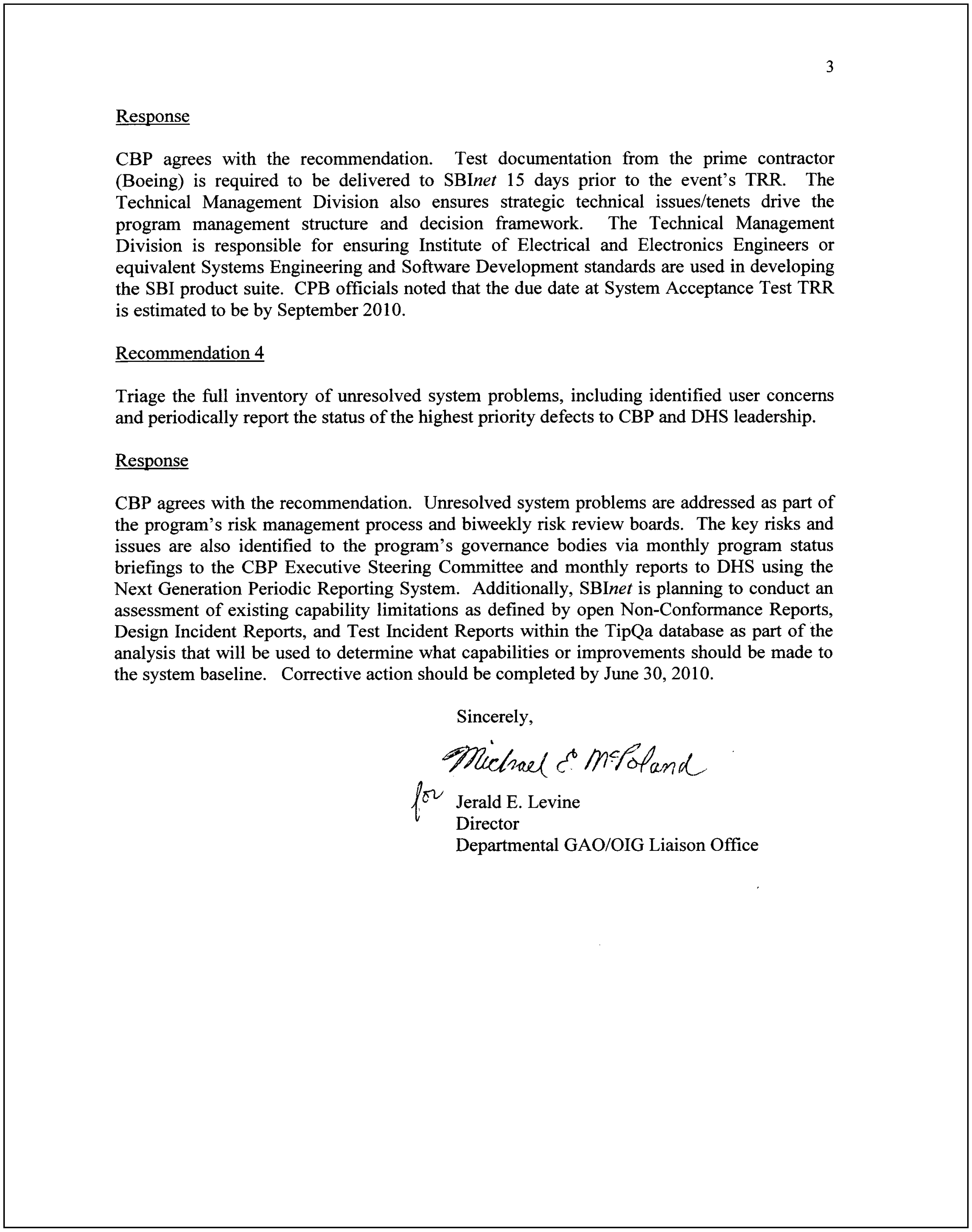
Ensure that test schedules, plans, cases, and procedures are adequately reviewed and approved consistent with the revised Test and Evaluation Master Plan.

Response

CBP agrees with the recommendation. Test artifacts are reviewed both in advance and at each test event's Test Readiness Review (TRR) to ensure alignment with the Program's Integrated Master Schedule, which incorporates changes to the approved Test and Evaluation Master Plan schedule. The SBI Systems Engineering (SE) Directorate was created to ensure systems engineering processes are being properly defined, executed, and monitored, the Technical Management Division within the SE Directorate is the entity responsible for ensuring verification and validation processes are being executed and system engineering best practices are being incorporated. CBP officials stated that the due date at System Acceptance Test (SAT) TRR is estimated to be by September 2010.

Recommendation 3

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



Response

CBP agrees with the recommendation. Test documentation from the prime contractor (Boeing) is required to be delivered to SBI*net* 15 days prior to the event's TRR. The Technical Management Division also ensures strategic technical issues/tenets drive the program management structure and decision framework. The Technical Management Division is responsible for ensuring Institute of Electrical and Electronics Engineers or equivalent Systems Engineering and Software Development standards are used in developing the SBI product suite. CPB officials noted that the due date at System Acceptance Test TRR is estimated to be by September 2010.

Recommendation 4

Triage the full inventory of unresolved system problems, including identified user concerns and periodically report the status of the highest priority defects to CBP and DHS leadership.

Response

CBP agrees with the recommendation. Unresolved system problems are addressed as part of the program's risk management process and biweekly risk review boards. The key risks and issues are also identified to the program's governance bodies via monthly program status briefings to the CBP Executive Steering Committee and monthly reports to DHS using the Next Generation Periodic Reporting System. Additionally, SBI*net* is planning to conduct an assessment of existing capability limitations as defined by open Non-Conformance Reports, Design Incident Reports, and Test Incident Reports within the TipQa database as part of the analysis that will be used to determine what capabilities or improvements should be made to the system baseline. Corrective action should be completed by June 30, 2010.

Sincerely,

Michael E. McFarland

for Jerald E. Levine
Director
Departmental GAO/OIG Liaison Office

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact named above, Deborah Davis (Assistant Director), Carl Barden, James Crimmer, Neil Doherty, Lauren Giroux, Nancy Glover, Dan Gordon, Lee McCracken, Sushmita Srikanth, and Jennifer Stavros-Turner made key contributions to this report.

(310674)

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