



**One Hundred Tenth Congress  
U.S. House of Representatives  
Committee on Homeland Security  
Washington, DC 20515**

Thursday, September 17, 2009

10:00 a.m. in 311 Cannon House Office Building

**Subcommittee on Border, Maritime, and Global Counterterrorism**

Hearing on

**“The Secure Border Initiative: SBInet Three Years Later”**

**WITNESSES**

**Chief David Aguilar**

U.S. Border Patrol  
U.S. Customs and Border Protection

**Mr. Mark Borkowski**

Executive Director  
Secure Border Initiative  
U.S. Customs and Border Protection

**Mr. Timothy E. Peters**

Vice President and General Manager  
Global Security Systems  
The Boeing Company

**Mr. Richard Stana**

Director  
Homeland Security and Justice Issues  
Government Accountability Office

**TESTIMONY OF**  
**DAVID AGUILAR**  
**CHIEF**  
**UNITED STATES BORDER PATROL**

**AND**

**MARK BORKOWSKI**  
**EXECUTIVE DIRECTOR, SECURE BORDER INITIATIVE**

**U.S. CUSTOMS AND BORDER PROTECTION**  
**DEPARTMENT OF HOMELAND SECURITY**

**BEFORE**

**HOUSE HOMELAND SECURITY COMMITTEE**  
**SUBCOMMITTEE ON BORDER, MARITIME, AND GLOBAL**  
**COUNTERTERRORISM**

**September 17, 2009**  
**Washington, DC**

Chairwoman Sanchez, Ranking Member Souder, and distinguished Members of the Subcommittee, it is a privilege and an honor to appear before you today to discuss “The Secure Border Initiative: SBInet Three Years Later.” At U.S. Customs and Border Protection (CBP), we are confident that we are making significant strides in our integrated efforts to increase the security of our borders.

I would like to start by emphasizing an important point: our border security efforts are integrated efforts, and while the Secure Border Initiative (SBI) is an important element of our overall strategy, it does not represent a panacea or a stand-alone capability for border security. It is one part of a much larger effort, which includes many stakeholders and partners across the federal government, as well as state, local, tribal, and international partners. The *National Southwest Border Counternarcotics Strategy*, released jointly this past June by Office of National Drug Control Policy Director Kerlikowske, Attorney General Holder, and Secretary Napolitano is one example of this broad, integrated effort.

The primary goal of our strategy between the ports of entry is to secure our Nation’s borders. This means consistently detecting illegal entries into the United States, assessing and classifying any threats associated with the illegal entries, responding to the area, and bringing the situation to a successful law enforcement resolution. Put a bit more simply, the ability to secure the border requires two basic conditions. First, we must have an accurate awareness of what is going on in the area around the border. Secondly, we must have the ability to respond to that awareness how, where, and when we deem it appropriate to respond. The ability to secure of the border, therefore, comes from a combination of both the knowledge and the ability to act on that knowledge.

In our view, control of our borders—particularly between the legal ports of entry—comes from an appropriate combination of personnel, technology, and tactical infrastructure. We often refer to this strategy as a “three-legged stool.” One of these legs alone cannot provide control of the border. The mix of these three elements will vary depending on the challenges of the focus area. Technology alone cannot control the borders, but it can provide a significant capability that augments and improves the effectiveness of an integrated approach. Similarly, tactical infrastructure, such as fencing, does not control the border independently of other elements.

How can we measure the effectiveness of each contribution (personnel, technology, and tactical infrastructure) to the overall control of the border? That is a difficult question to answer. No one of the elements that contribute to border control can do the job without contributions from the other elements. For example, we cannot say that fencing prevented a discrete number of people from crossing the border illegally, and that technology prevented some others, and personnel prevented still others. In fact, even to ask the question perpetuates the misperception that any single one of these elements can control the border.

We do believe, however, that we can evaluate and characterize the effectiveness of our integrated efforts to secure the border. And we can characterize the contribution of

each of the three legs of the stool even if we cannot precisely quantify the individual contribution of each component. Technology allows us to detect the entries and to assess and classify the threat. Personnel provide the response to confront the criminal element. Tactical infrastructure supports the response by either providing access or extending the time needed for the response by deterring or slowing the criminal element's ability to easily cross the border and escape.

Personnel are the most flexible and robust of the elements, since they can provide both knowledge (through observation) and response. However, use of personnel alone is not the most efficient way to achieve border control. Deploying enough personnel to provide 24/7 coverage of large areas of the border would be cost prohibitive as well as a nonsensical use of funds. Technology can be used to "watch" large areas of the border, thus helping with the "knowledge" part of the equation. By using technology in this role, we can relieve personnel of the requirement to stand and observe, and redeploy them to serve where current technology cannot – in the area of response. Finally, we can use tactical infrastructure, such as fencing, as a fixed resource to deter and delay illicit cross-border incursions. It is important to recognize that tactical infrastructure and technology are not interchangeable. Infrastructure (including fencing) provides a constant and continuous effect, and more options for response. I wish to be very clear—fence alone does not and cannot provide effective control of the border. It does, however, provide a continuous and constant ability to deter or delay, which we refer to as "persistent impedance." That delay provides more time for personnel to respond to the incursion, but it cannot altogether stop an incursion.

The current focus of SBI is to support border control efforts by providing tactical infrastructure and technology. SBInet, which is the primary focus of this hearing, represents the technology contribution of SBI. Before discussing the details of SBInet, it might be useful to provide a short update on our progress with respect to construction of the fence along the southwest border. As of the end of August, we have approximately 632 miles of fence constructed. Of that, approximately 334 miles are pedestrian fence and the remaining 298 miles are vehicle fence. Our target, based on Border Patrol's operational assessments of fencing needs, has been approximately 670 miles. The exact total mileage is imprecise at this point because it will depend on the actual measurement of completed fence as opposed to pre-construction estimates. The fence that is not yet complete is still planned but has been delayed primarily due to legal proceedings related to the condemnation and transfer of real estate required for the fence.

As already noted, fence provides persistent impedance, which contributes to our ability to secure the border by providing additional time for agents to respond to incursions. There are locations where the Border Patrol has concluded that persistent impedance is absolutely necessary in order to gain control of the border. There are other areas where persistent impedance would be a useful contribution but it is not an absolute necessity. It is important to emphasize the fact that we have constructed and planned fencing in areas where the Border Patrol has concluded that persistent impedance is a *necessity*; we have *not* built fence in areas where we think we might be able to achieve control through other means—that is, through different combinations of personnel,

technology, and tactical infrastructure—or where we have encountered engineering or other challenges in moving forward with construction. Before any consideration is given to building fencing in other locations, we want to ensure that CBP has determined the operational requirements for effective control in those areas, and has the opportunity to compare any other options we can identify. An accurate assessment requires more experience and observation, both in areas where we have fencing and in areas where we do not, so that we have a good basis for the comparison.

Furthermore, we have built fence where we have concluded it is the most cost-effective way to provide persistent impedance. As a practical matter, the only other, albeit unrealistic, way to provide persistent impedance is to deploy personnel fairly densely along the border, in fixed locations, twenty-four hours a day and seven days a week. We reviewed these options in a set of detailed “Analyses of Alternatives,” which we have provided to the Congress as part of our annual expenditure plan.

Let me now turn to some specifics about SBInet, the technology part of SBI, which is the focus of this hearing. The SBInet program is focused on developing and deploying a system of networked sensor towers that can provide surveillance and situational awareness over stretches of the border. The SBInet system will be deployed in discrete Areas of Responsibility (AoRs), each of which covers a length of border ranging between approximately 20 and 40 miles. The basic concept involves constructing towers in locations that are selected based on knowledge of terrain, vegetation, and typical routes used by illegal entrants, as well as by sensitivity to and impact on the environment. Each of the sensor towers in an AoR includes a ground surveillance radar, a day camera, and a night camera. Each also includes a receiver for signals from unattended ground sensors (UGSs), which are hidden within the AoR and can detect nearby movement. There are also communications relay towers, which receive the signals from the sensor towers and transmit them back to a Border Patrol station. One key element of SBInet that distinguishes it from other technology at the border is the networking of the towers and sensors. Information from the various cameras, radars, and sensors is combined within a computer system called the Common Operating Picture (COP). The COP provides a display on computer monitors that includes an integrated picture of the radar and sensor detections from all of the towers within an AoR. It also provides the feeds from the day and night cameras, and software that can point the cameras in order to look at what the radars and sensors have detected.

Project 28 was our initial effort to prototype this type of SBInet system. As a prototype, we did not intend Project 28 to be the actual system we would put in production. We did, however, anticipate that, even as a prototype, Project 28 would provide us with improved capability, and we advertised that it would be a relatively simple and low risk effort. Unfortunately, it did not work as well as we anticipated and took longer than it should have to complete. But we learned from the experience and we are in the process of making significant improvements.

Since the initial experience, we have improved Project 28 to the point that it is currently operational and effective in supporting the Border Patrol in the area around

Sasabe, Arizona. Border Patrol agents credit Project 28 with providing them with enhanced situation awareness that has assisted in the detection and subsequent apprehension of over 5,000 illegal entrants and the interdiction of over 14,000 pounds of marijuana. Without Project 28—and absent some other increase in capability, such as more agents—the success rate of these apprehensions and interdictions may have been lower.

Our SBInet contractor, Boeing, has taken a great deal of criticism for its past performance on SBInet. In truth, SBI has not been fully satisfied with Boeing's performance to date. It is worth noting, however, that Boeing delivered Project 28 on a firm fixed price task order basis and absorbed tens of millions of dollars in losses in order to correct the initial deficiencies, demonstrating a significant commitment to deliver a useful capability.

We were able to use the lessons we learned from Project 28 to design the first generation of the operational SBInet system. We call this first generation SBInet Block 1. We have completed most of the engineering design of SBInet Block 1 and have performed extensive engineering testing. Although the engineering tests increased our overall confidence in the system, they did identify some areas for improvement. We do not believe those areas represent “show stoppers,” but we have taken steps to enforce a deliberative and disciplined process to address them, including opting to delay some program activities while we await the results of further testing and analysis.

At this point, we are in the process of doing our first deployment into an operational AoR, known as Tucson-1, (Tus-1). Tus-1 will replace Project 28 (the prototype system) with the new Block 1 (first generation production system) to cover 23 miles of border around Sasabe, Arizona. Tus-1 includes nine sensor towers and eight communications relay towers, all of which are now constructed. We are now starting basic system and component checkout of the Tus-1 systems and awaiting results of some remaining corrective actions before authorizing Boeing to begin more comprehensive system testing. SBI anticipates being prepared to provide that authorization within the next few weeks, at which point we will conduct extensive engineering tests on the system. Those tests are designed to demonstrate that the system meets its engineering requirements. If it passes, SBI will accept the system from Boeing.

Provided SBI accepts it, the Border Patrol will receive the system, probably in early January, to conduct a formal process known as Operational Test and Evaluation (OT&E). In OT&E, the Border Patrol will conduct disciplined assessments in a real world environment to determine whether the SBInet Block 1 system is effective and suitable for use. Based on these assessments, the Border Patrol will effectively deliver a report card to SBI, indicating whether or not it has met their operational requirements. The Border Patrol is still designing the test regimen, but we anticipate OT&E will continue at least into March of next year.

While testing is underway, we expect to begin the deployment of our second AoR, known as “Ajo-1.” Ajo-1 will cover about 30 miles of border near Ajo, Arizona.

Our experience with Ajo-1 will build on Tus-1 and ensure we can move from one deployment activity to another in a smooth and effective manner. Ajo-1 should be completed and tested by late spring or early summer of next year.

Taken together, Tus-1 and Ajo-1 represent the initial deployment of Block 1. Through its structured review process, the Department of Homeland Security (DHS) has authorized initial deployment—but not full deployment. This is a normal sequence of events. Before authorizing full deployment, we need to have the results of the Border Patrol’s OT&E and demonstrate that we can effectively and efficiently complete the deployment process. As currently planned, full deployment of Block 1 means deployment along the Arizona border. The exact schedule for that deployment will depend on the successful completion of initial deployment activities, as well as other decisions that will be advised by the initial deployments. For example, based on results from the initial deployments, CBP will gain experience and knowledge about how well SBInet contributes to the technology element of border control. With that knowledge, we can make better decisions about where it is most cost-effective to use SBInet Block 1. CBP will also have better information about the desired pace of deployments going forward and can reflect those decisions in future budget submissions.

In short, we believe we are making appropriate progress towards the deployment of SBInet Block 1. Based on the testing that has been performed to date, we have a sound level of engineering confidence that the system will meet its requirements. In order to increase our confidence, we are proceeding with the initial deployments and the formal OT&E process.

We have set requirements for our program that are modest but effective. Remembering that technology does not, in and of itself, control the border, we require SBInet Block 1 to detect at least 70 percent of incursions within each AoR and provide accurate identification at least 70 percent of the time. The Subcommittee may recall that early goals for SBInet were at 95 percent, rather than the 70 percent we have currently established. This threshold does not indicate that we will allow failure to detect or identify incursions 30 percent of the time. Rather, we recognize that the SBInet system is one contribution among several resources we have available, such as air assets, tactical infrastructure, additional technology, and personnel. Based on experience, cost, and a better understanding that the role of technology is to contribute, SBInet’s contribution may well be adequate to provide an overall, integrated capability of 95 percent or more, when all of the other elements of border control are taken into account.

In designing the Block 1, we have selected modest components which we believe are cost-effective and anticipate will do the job. While there are other cameras and radars that are higher performing, by starting with the currently-designed Block 1, we: avoid the risk of over-designing; we reduce the risk of excessive cost, schedule, and technical problems; we provide an operational capability sooner; and we provide the quickest possible opportunity to evaluate the effectiveness of the system in an operational environment. With some real-world experience, we can make future decisions about how and if we should enhance the system. Our block approach to SBInet, which represents an

acquisition strategy known as spiral development, provides us an opportunity to deliver cost-effective enhancements in the future, as needed or desired.

While we are deploying the SBInet Block 1 system and tightening up our requirements discipline, we are also taking steps to improve our competence in the management of complex acquisition programs. We have redesigned our SBI organization to develop and retain skilled government personnel in the disciplines that are key to successful program management. We are also strengthening our oversight and management of our contractors' activities to ensure we are able to communicate our requirements clearly and consistently.

We are strengthening the role and influence of the end users of our systems—in this case, the Border Patrol—in the development and acquisition process. The structured OT&E we described, which is a normal process in the Department of Defense but relatively new to us, is one example. Beyond that, operational end users participate in overseeing program activities, setting priorities, and deciding on acquisition courses of action. End users also now have a more structured process and conduit to request consideration of program changes, and to participate in trade-offs between capabilities and costs.

We are eager to establish better ways to predict and evaluate the effectiveness of our systems. We are confident that increased enforcement efforts have had a positive effect on our ability to control our borders. Since 2006, we have increased the size of the Border Patrol from approximately 12,350 agents to nearly 20,000 today. We now have almost 650 miles of fence deployed to areas along the border where we need it most. And we have begun to deploy effective technology to critical areas. There is no question, based on the measures we have available, that these enforcement activities have reduced illegal activity between the ports of entry.

Going forward, we acknowledge we need to find a better way to characterize and measure the effects of increased enforcement. The third party indicators we currently use, like trends in apprehensions or drug seizures, taken with our subject matter expert assessment about relative levels of border control, are useful and valid. But we still need to develop tools that will allow us to assess different mixes of personnel, tactical infrastructure, and technology; to compare their effectiveness; and to compare their costs. In this way, we can make better decisions about the most cost-effective investments. In order to develop the appropriate tools, we need to gain experience and measure results of our ongoing efforts. We believe we are headed in that direction with our current activities.

In closing, although we know that the last three years of SBInet have been frustrating and at times discouraging for all involved, we believe we are on a path towards improvement. We thank Congress and this Subcommittee for your interest in this issue and share your desire for the achievement of results. We appreciate the Subcommittee's continued support of CBP's efforts to better secure our borders and look forward to responding to your questions.

**Statement of**

**Mr. Timothy E. Peters  
Vice President, Global Security Systems  
The Boeing Company**

**On**

**The Secure Border Initiative: *SBI*net Three Years Later**

**Before the  
Committee on Homeland Security  
Subcommittee on Border, Maritime and Global  
Counterterrorism**

**U.S. House of Representatives**

**September 17, 2009**

I'm Tim Peters, Vice President of Boeing's Global Security Systems, which includes the *SBI*net program. I appreciate the opportunity to discuss progress on *SBI*net before the Subcommittee on Border, Maritime, and Global Counterterrorism.

Today, I'll address our progress in designing and developing the overall *SBI*net solution. I'll also update you on the deployment status of Block 1, which is based on the same concept of integrated, commercial technology, but includes improvements from P-28. I'll also say a few words about activities on the Northern Border.

### **P-28 Lessons Learned**

P-28 has proven to be a valuable operational tool for the Border Patrol, as well as a framework for development of Block 1 and future *SBI*net systems. Operational for eighteen months, P-28 has been instrumental in apprehension of thousands of illegal border crossers and interception of thousands of pounds of narcotics, according to recent Customs and Border Protection reports. Many important lessons learned from the prototype P-28 system have been incorporated into the development of Block 1, including:

- Active involvement of the entire user community in the system design and function;
- Laboratory testing of components, systems and subsystems, and the creation of an operationally representative test-bed for field testing; and
- A substantially improved Common Operating Picture.

### **Block 1**

The Block 1 system has been in development for the past two years. The first deployment is known as Tucson 1 – or TUS-1 – is now well along in the P-28 area of operations and will cover 23 miles of the border around the Sasabe Port of Entry. A second deployment, called AJO-1, has been initiated west of the TUS-1 area of operations and will cover 30 miles of border at the

Lukeville Port of Entry. AJO-1 construction will follow TUS-1 by several months while we await the Department of the Interior's environmental approval.

TUS-1 consists of nine sensor towers and eight communications towers. Of the 17 total towers, Boeing built 13 new towers and modified four existing government towers. As of today, all tower construction is complete, and all sensors have been installed. For those of you familiar with the system, it has a distinctly different look to complement its improved capabilities. We are using a fixed tower, an upgraded sensor package, a different support equipment package, and most importantly, greatly improved communication technology. Specifically, TUS-1 and all future deployments will send data back to sector headquarters via a line-of-sight microwave link or fiber-optic link where it is available or not cost-prohibitive to do so. Gone are the satellite dishes used in the P-28 system, as well as the system lags they produced. The TUS-1 system is much more responsive, providing information to agents more quickly. The new Common Operating Picture (or COP) software is also responsible for significant improvements in responsiveness and usability. Boeing engineers sat side-by-side with Border Patrol agents who served as the primary designers of the look, feel and function of the Block 1 COP.

While we've encountered some technological challenges – not uncommon when integrating off-the-shelf components – we're working diligently within our team and the customer to resolve issues quickly and thoroughly, so the operational system will be robust and reliable. There have been two recent issues that have been particularly problematic – radar control, and human-machine interface malfunctions. I'm happy to report that we have implemented solutions to address each of those problems. We've been testing these solutions for several weeks, and the problems have not recurred.

Once these solutions are fully implemented over the coming weeks, the Block 1 system will complete System Qualification Test (SQT) at test facilities in Playas, New Mexico, then the deployed TUS-1 system will undergo Systems Acceptance Testing (SAT) during the fourth quarter this year. When completed, we'll hand the system over to the government for Operational Testing and Evaluation (OT&E), which will be overseen by the Border Patrol. Results of these

tests will assist the customer in determining future deployments, system enhancements and designs for other border geographies.

### **AJO-1**

The AJO-1 deployment is also progressing well. System design is complete, and the command-and-control facility is already under construction. The majority of the hardware has been purchased, and site work and installation are awaiting environmental approval from the Department of the Interior, expected in mid-October. The AJO deployment consists of six sensor towers and five communications towers, spanning about 30 miles of border.

### **Northern Border**

The Boeing team has also been active on the Northern Border with projects in the Detroit and Buffalo Sectors. Boeing is installing Remote Video Surveillance Systems, or RVSS, to enhance surveillance capabilities in a cold-weather, river environment. The RVSS are comprised of two sets of day and night cameras atop monopoles or existing structures. These systems feed video images back to sector headquarters using the same microwave communications design as being deployed in TUS-1 on the southwest border. However, in this deployment we aren't including radar for additional detection or a Common Operational Picture for multi-sensor correlation and tracking. Eleven RVSS are slated to be installed in the Detroit Sector to monitor activities along the St. Clair River and five in the Buffalo Sector to monitor activities along the Upper Niagara River. Installation began in the Buffalo Sector in May, and efforts recently started in the Detroit Sector. We expect both projects to be fully operational by early 2010.

### **Conclusion**

In conclusion, let me say that *SBI*net has been both a challenging and also an important program to The Boeing Company. The Project 28 prototype and Block 1 system, which have received a

majority of the attention, represent approximately half of the government-funded effort to date. Boeing has invested its own funds in *SBI<sub>net</sub>*: we built a systems integration lab in Huntsville, Alabama; we established the Rapid Application Development / Joint Application Development lab in Arlington, Virginia; and we created modeling and simulation tools to support development. These have been significant factors in the program's success to date. Boeing has also leveraged existing capabilities to support *SBI<sub>net</sub>*. For example, the entire TUS-1 network was replicated in our existing Network Systems Integration Laboratory (NSIL) in El Segundo, California, to ensure it was operationally robust prior to deployment.

Boeing's support to Customs and Border Protection has extended beyond *SBI<sub>net</sub>*. Last year, we supported tactical infrastructure efforts through the Supply and Supply Chain Management task order. Using our supply chain expertise, we procured more than \$440 million or 140,000 tons of steel for use in 290 miles of fence construction. That's the equivalent of three modern-day aircraft carriers. According to September 2008 testimony by then-U.S. Customs and Border Protection Commissioner W. Ralph Basham, between \$63 million and \$100 million was saved.

Our goal has been to provide a complete system, technology and tools to bolster security for the nation, increase agent safety and add value for taxpayers. With the Tucson deployment underway, *SBI<sub>net</sub>* now has a baseline to be replicated in future deployments, such as AJO-1. We have a frame of reference from an operational deployment, not just the prototype of Project 28. The Block 1 system remains the core of our effort, and I believe our work over the last few years has lowered risk and increased system integrity. I also believe our work has produced a capability that will give the Border Patrol agents a highly effective tool to enhance border security and improve agent safety. We have now had the opportunity to work in the field with the Border Patrol Agents and have a more thorough understanding of the challenges they are facing. We believe that the Block 1 system architecture we are providing, once deployed, is readily scalable and upgradeable to incorporate new and improved sensors to meet changes in the Border Patrol Agent's mission.

Thank you for the opportunity to testify. I look forward to your questions.

**GAO**

Testimony

Before the Subcommittee on Border,  
Maritime and Global Counterterrorism,  
Committee on Homeland Security, House  
of Representatives

---

For Release on Delivery  
Expected at 10:00 a.m. EDT  
Thursday, September 17, 2009

# SECURE BORDER INITIATIVE

## Technology Deployment Delays Persist and the Impact of Border Fencing Has Not Been Assessed

Statement of Richard M. Stana, Director  
Homeland Security and Justice Issues



**GAO**

Accountability \* Integrity \* Reliability

---

---

Chairwoman Sánchez, Ranking Member Souder, and Members of the Subcommittee:

I am pleased to be here today to discuss the implementation of the Department of Homeland Security's (DHS) Secure Border Initiative (SBI) program—a multiyear, multibillion dollar program aimed at securing U.S. borders and reducing illegal immigration. Securing the nation's borders from illegal entry of aliens and contraband, including terrorists and weapons of mass destruction, continues to be a major challenge. In November 2005, DHS announced the launch of SBI to help address this challenge. The U.S. Customs and Border Protection (CBP) supports this initiative by providing agents and officers to patrol the borders, secure the ports of entry, and enforce immigration laws.<sup>1</sup> In addition, CBP's SBI program is responsible for developing a comprehensive border protection system using technology, known as *SBI<sub>net</sub>*, and tactical infrastructure—fencing, roads, and lighting—along the southwest border to deter smugglers and aliens attempting illegal entry.<sup>2</sup> Since fiscal year 2005, SBI has received funding amounting to over \$3.7 billion. Approximately \$1.1 billion has been allocated to *SBI<sub>net</sub>* and \$2.4 billion to tactical infrastructure.<sup>3</sup>

*SBI<sub>net</sub>* surveillance technologies are to include sensors, cameras, and radars. The command, control, communications, and intelligence (C3I) technologies are to include software and hardware to produce a Common Operating Picture (COP)—a uniform presentation of activities within specific areas along the border. *SBI<sub>net</sub>* technology is to be initially deployed in two geographic areas—designated as Tucson-1 and Ajo-1—within the Tucson sector.<sup>4</sup> In September 2006, CBP awarded a prime

---

<sup>1</sup>At a port of entry location, CBP officers secure the flow of people and cargo into and out of the country, while facilitating legitimate travel and trade.

<sup>2</sup>The SBI Program Executive Office, referred to in this testimony as the SBI program office, has overall responsibility for overseeing all SBI activities for acquisition and implementation, including establishing and meeting program goals, objectives, and schedules for overseeing contractor performance, and for coordinating among DHS agencies. However, as of March 2009, the tactical infrastructure program office was realigned and is now managed on a day-to-day basis by CBP's Office of Finance Facilities Management and Engineering division.

<sup>3</sup>Remaining funds were allocated to program management and environmental requirements.

<sup>4</sup>The U.S. Border Patrol has 20 sectors in which it is responsible for detecting, interdicting, and apprehending those who engage in illegal activity across U.S. borders between official ports of entry.

---

contract for *SBI*net development to the Boeing Company for 3 years, with three additional 1-year options. As of July 8, 2009, CBP had awarded 13 task orders to Boeing for a total amount of approximately \$1.1 billion.<sup>5</sup>

In addition to deploying technology across the southwest border, DHS planned to deploy 370 miles of single-layer pedestrian fencing and 300 miles of vehicle fencing by December 31, 2008. Pedestrian fencing is designed to prevent people on foot from crossing the border and vehicle fencing consists of physical barriers meant to stop the entry of vehicles. In September 2008, DHS revised its goal, committing instead to having 661 miles either built, under construction, or under contract by December 31, 2008, but did not set a goal for the number of miles it planned to build by December 31, 2008. Although some tactical infrastructure exists in all the southwest border sectors, most of what has been built through the *SBI* program is located in the San Diego, Yuma, Tucson, El Paso, and Rio Grande Valley sectors.

My testimony is based on a report we are publicly releasing today<sup>6</sup> that is the fourth in a series of interim reports on *SBI* implementation.<sup>7</sup> My testimony will discuss the following key issues in our report: (1) the extent to which CBP has implemented the *SBI*net technology program and the impact of any delays that have occurred, and (2) the extent to which CBP has deployed the *SBI* tactical infrastructure program and assessed its results. Our full report also provides a status of *SBI* program office staffing and the progress the office reports in achieving its human capital goals. I will conclude with some observations regarding our recommendation and DHS's response.

For our report, we reviewed program schedules, status reports, and previous GAO work and interviewed DHS and CBP officials, including representatives of the *SBI* program office and the tactical infrastructure

---

<sup>5</sup>See appendix II of our September 2009 report—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)—for a summary of the task orders awarded to Boeing for *SBI* projects.

<sup>6</sup>[GAO-09-896](#).

<sup>7</sup>GAO, *Secure Border Initiative: Observations on Selected Aspects of SBI*net Program Implementation, [GAO-08-131T](#) (Washington, D.C.: Oct. 24, 2007); *Secure Border Initiative: Observations on the Importance of Applying Lessons Learned to Future Projects*, [GAO-08-508T](#) (Washington, D.C.: Feb. 27, 2008); and *Secure Border Initiative: Observations on Deployment Challenges*, [GAO-08-1141T](#) (Washington, D.C.: Sept. 10, 2008); [GAO-09-896](#).

---

program office; the Border Patrol (a component of CBP); and the Department of Interior (DOI). We visited three SBI sites where *SBI*net technology (Project 28) and/or fencing had been deployed at the time of our review.<sup>8</sup> We determined that funding, staffing, and fencing mileage data provided by CBP were sufficiently reliable for the purposes of our report. More detailed information on our scope and methodology appears in our September 2009 report. Our work was performed in accordance with generally accepted government auditing standards.

---

## ***SBI*net Continues to Experience Delays, and Border Patrol Continues to Rely on Existing Technology That Has Limitations That Newer Technology Is Planned to Overcome**

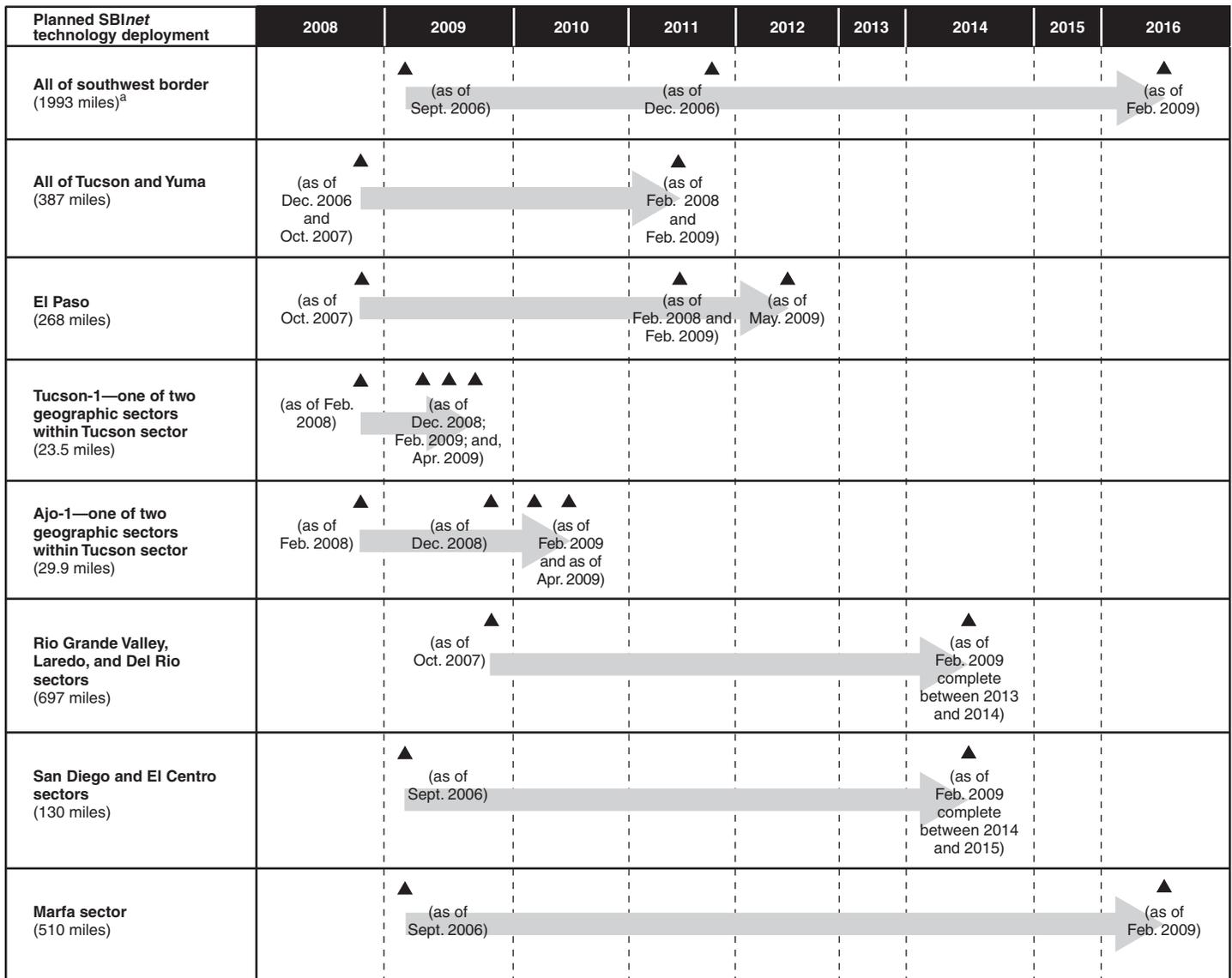
*SBI*net technology capabilities have not yet been deployed and delays require the Border Patrol to rely on existing technology for securing the border, rather than using newer technology planned to overcome the existing technology's limitations. As of September 2006, *SBI*net technology deployment for the southwest border was planned to be complete in fiscal year 2009. When last reported in February 2009, the completion date had slipped to 2016. In addition, by February 2009, the schedule for Tucson-1 and Ajo-1 had slipped from the end of calendar year 2008, and final acceptance of Tucson-1 was expected in November 2009 and Ajo-1 in March 2010. As of April 2009, Tucson-1 was scheduled for final acceptance by December 2009 and Ajo-1 had slipped to June 2010.<sup>9</sup> (See fig. 1 for schedule changes over time).

---

<sup>8</sup>Project 28 was an effort to provide a technology system with the capabilities to control 28 miles of the border in Arizona.

<sup>9</sup>The SBI program office defines final acceptance as the SBI program office taking ownership of the *SBI*net technology system from the contractor and comes before handing the technology over to Border Patrol.

**Figure 1: Depiction of Changes in the SBInet Deployment Schedule from September 2006 through May 2009**



▲ Estimated completion date

Source: CBP's SBI program office and Border Patrol.

<sup>a</sup>Miles represent the area of responsibility of the sector(s).

Flaws found in testing and concerns about the impact of placing towers and access roads in environmentally sensitive locations caused delays. By February 2009, preliminary results of testing revealed problems that may

---

limit the usefulness of the system for Border Patrol agents, including the instability of the camera under adverse weather conditions, mechanical problems with the radar at the tower, and issues with the sensitivity of the radar. As of May 2009, the SBI program office reported that they were still working with Boeing to address some issues such as difficulties aligning the radar.

As a result of the delays, Border Patrol agents continue to use existing technology that has limitations, such as performance shortfalls and maintenance issues. For example, on the southwest border, the Border Patrol relies on existing equipment such as cameras mounted on towers that have intermittent problems, including signal loss. The Border Patrol has procured and delivered some new technology to fill gaps or augment existing equipment. However, incorporating *SBI<sub>net</sub>* technology as soon as it is operationally available should better position CBP to identify and implement operational changes needed for securing the border.

---

## Tactical Infrastructure Deployments Are Almost Complete, but Their Impact on Border Security Has Not Been Measured

Tactical infrastructure deployments are almost complete, but their impact on border security has not been measured. As of June 2009, CBP had completed 633 of the 661 miles of fencing it committed to deploy along the southwest border (see table 1). However, delays continue mainly because of challenges in acquiring the necessary property rights from landowners. While fencing costs increased over the course of construction, because all construction contracts have been awarded, costs are less likely to change. CBP plans to use \$110 million in fiscal year 2009 funds to build 10 more miles of fencing, and fiscal year 2010 and 2011 funds for supporting infrastructure. The life-cycle cost study prepared by a contractor for CBP shows that total 20-year life-cycle costs are estimated at about \$6.5 billion for all tactical infrastructure—including pre-SBI infrastructure as well as that planned for fiscal years 2009, 2010, and 2011—and consisting of deployment and operations and future maintenance costs for the fence, roads, and lighting, among other things.

**Table 1: Tactical Infrastructure Deployment Progress as of June 26, 2009**

<b>Infrastructure type</b>	<b>Miles in place before SBI<sup>a</sup></b>	<b>Miles deployed through SBI as of 6/26/09</b>	<b>Total miles in place as of 6/26/09</b>	<b>Target</b>	<b>Miles remaining to meet target</b>
Pedestrian fencing	67	264	331	358	27
Vehicle fencing	76	226	302	303	1
<b>Total fencing</b>	<b>143</b>	<b>490</b>	<b>633</b>	<b>661</b>	<b>28</b>

Source: GAO analysis of SBI data.

<sup>a</sup>Seventy-eight miles of pedestrian fencing and 57 miles of vehicle fencing were in place before the SBI program began. However, since SBI began construction, some miles of fencing have been removed, replaced or retrofitted resulting in mileage totals that are different from those we have reported in earlier reports.

CBP reported that tactical infrastructure, coupled with additional trained agents, had increased the miles of the southwest border under control, but despite a \$2.4 billion investment, it cannot account separately for the impact of tactical infrastructure. CBP measures miles of tactical infrastructure constructed and has completed analyses intended to show where fencing is more appropriate than other alternatives, such as more personnel, but these analyses were based primarily on the judgment of senior Border Patrol agents. Leading practices suggest that a program evaluation would complement those efforts.<sup>10</sup> Until CBP determines the contribution of tactical infrastructure to border security, it is not positioned to address the impact of this investment. In our report, we recommended that to improve the quality of information available to allocate resources and determine tactical infrastructure’s contribution to effective control of the border, the Commissioner of CBP conduct a cost-effective evaluation of the impact of tactical infrastructure on effective control of the border.

DHS concurred with our recommendation and described actions recently completed, under way, and planned that the agency said will address our recommendation. For example, DHS commented that it is considering using independent researchers to conduct evaluations and considering using modeling and simulation technology to gauge the effects of resource deployments. We believe that such efforts would be consistent with our

<sup>10</sup> In program evaluation, scientific research methods are used to establish a causal connection between program activities and outcomes and to isolate the program’s contributions to them. GAO, *Program Evaluation: Studies Helped Agencies Measure or Explain Program Performance*, GAO/GGD-00-204 (Washington, D.C.: Sept. 2000).

---

recommendation, further complement performance management initiatives, and be useful to inform resource decision making.

---

This concludes my prepared testimony. I would be pleased to respond to any questions that members of the subcommittee may have.

---

## Contacts and Acknowledgments

For further information regarding this testimony, please contact Richard M. Stana at (202) 512-8777 or [stanar@gao.gov](mailto:stanar@gao.gov). In addition, contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals who made key contributions to this testimony are Assistant Director Susan Quinlan, Sylvia Bascopé, and Katherine Davis.

---

---

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

---

## 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](http://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](http://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](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Ralph Dawn, Managing Director, [dawnr@gao.gov](mailto: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](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548

