United States Senate
COMMITTEE ON FINANCE
WASHINGTON, DC 20510-6200

June 12, 2008

**Via Electronic Transmission**

W. Ralph Basham
Commissioner
U.S. Customs and Border Protection
1300 Pennsylvania Avenue, NW
Washington, DC 20229

Dear Commissioner Basham:

In August 2006, the Finance Committee held a hearing at which was demonstrated commercially available technology that, if placed at primary inspection points, could allow for the rapid detection of multiple forms of false identification used by travelers seeking to enter the United States. At the hearing, the machines successfully detected the false drivers licenses used by GAO investigators to cross into the United States in a matter of seconds. The technology appeared to be faster and more accurate than a trained officer attempting to detect false identification merely through human inspection of the document.

It has been two years since we urged Customs and Border Protection to examine and consider deploying such technology at primary inspection points in order to detect and deter terrorists and criminals from simply using false identification and a claim of U.S. citizenship to walk right through America's front door. Please provide the Committee with detailed written responses to the following questions:

1. What steps have you taken in the last two years to examine and evaluate the type of technologies demonstrated at the Committee's August 2006 hearing?

2. What percentage of primary inspection points at land ports of entry have installed new technology in the last two years to assist with the detection of false identification? If any, please describe the nature of the new technology.

Please provide your response by June 27, 2008. If you have any questions about this request, please contact John Angell of Chairman Baucus's staff or Jason Foster of Senator Grassley's staff at (202) 224-4515.

Sincerely,

Max Baucus
Chairman

Charles E. Grassley
Ranking Member

Attachment

United States Government Accountability Office

GAO

Report to the Committee on Finance, U.S. Senate

May 2008

# BORDER SECURITY

# Summary of Covert Tests and Security Assessments for the Senate Committee on Finance, 2003–2007

**This Report Is Temporarily Restricted Pending Official Public Release.**

G A O

Accountability * Integrity * Reliability

GAO-08-757

May 2008

GAO
Accountability • Integrity • Reliability
Highlights

Highlights of GAO-08-757, a report to the Committee on Finance, U.S. Senate

# BORDER SECURITY

## Summary of Covert Tests and Security Assessments for the Senate Committee on Finance, 2003–2007

### Why GAO Did This Study

From January 2003 to September 2007, GAO testified before the Committee on three occasions to describe security vulnerabilities that terrorists could exploit to enter the country. GAO's first two testimonies focused on covert testing at ports of entry—the air, sea, and land locations where international travelers can legally enter the United States. In its third testimony, GAO focused on limited security assessments of unmanned and unmonitored border areas between land ports of entry.

GAO was asked to summarize the results of covert testing and assessment work for these three testimonies. This report discusses the results of testing at land, sea, and air ports of entry; however, the majority of GAO's work was focused on land ports of entry. The unmanned and unmonitored border areas GAO assessed were defined as locations where the government does not maintain a manned presence 24 hours per day or where there was no apparent monitoring equipment in place. GAO assessed a nonrepresentative selection of these locations and did not attempt to evaluate all potential U.S. border security vulnerabilities. Further, GAO's work was limited in scope and cannot be projected to represent systemic weaknesses.

In response to this report, DHS provided a written update on numerous border protection efforts it has taken to enhance border security since 2003. GAO did not attempt to verify the information provided by DHS, but has included the response in this report.

To view the full product, including the scope and methodology, click on GAO-08-757. For more information, contact Gregory D. Kutz at (202) 512-6722 or kutzg@gao.gov.

### What GAO Found

GAO investigators identified numerous border security vulnerabilities, both at ports of entry and at unmanned and unmonitored land border locations between the ports of entry. In testing ports of entry, undercover investigators carried counterfeit drivers' licenses, birth certificates, employee identification cards, and other documents, presented themselves at ports of entry and sought admittance to the United States dozens of times. They arrived in rental cars, on foot, by boat, and by airplane. They attempted to enter in four states on the northern border (Washington, New York, Michigan, and Idaho), three states on the southern border (California, Arizona, and Texas), and two other states requiring international air travel (Florida and Virginia). In nearly every case, government inspectors accepted oral assertions and counterfeit identification provided by GAO investigators as proof of U.S. citizenship and allowed them to enter the country. In total, undercover investigators made 42 crossings with a 93 percent success rate. On several occasions, while entering by foot from Mexico and by boat from Canada, investigators were not even asked to show identification. For example, at one border crossing in Texas in 2006, an undercover investigator attempted to show a Customs and Border Protection (CBP) officer his counterfeit driver's license, but the officer said, "That's fine, you can go" without looking at it. As a result of these tests, GAO concluded that terrorists could use counterfeit identification to pass through most of the tested ports of entry with little chance of being detected.

In its most recent work, GAO shifted its focus from ports of entry and primarily performed limited security assessments of unmanned and unmonitored areas between ports of entry. The names of the states GAO visited for this limited security assessment have been withheld at the request of CBP. In four states along the U.S.–Canada border, GAO found state roads that were very close to the border that CBP did not appear to monitor. In three states, the proximity of the road to the border allowed investigators to cross undetected, successfully simulating the cross-border movement of radioactive materials or other contraband into the United States from Canada. For example, in one apparently unmanned, unmonitored area on the northern border, the U.S. Border Patrol was alerted to GAO's activities through the tip of an alert citizen. However, the responding U.S. Border Patrol agents were not able to locate the investigators and their simulated contraband. Also on the northern border, GAO investigators located several ports of entry in one state on the northern border that had posted daytime hours and were unmanned overnight. Investigators observed that surveillance equipment was in operation, but that the only preventive measure to stop an individual from crossing the border into the United States was a barrier across the road that could be driven around. GAO also identified potential security vulnerabilities on federally managed lands adjacent to the U.S.–Mexico border. GAO concluded that CBP faces significant challenges on the northern border, and that a determined cross-border violator would likely be able to bring radioactive materials or other contraband undetected into the United States by crossing the U.S.–Canada border at any of the assessed locations.

# Contents

**Letter** 1

Results in Brief 3
Background 5
Security Vulnerabilities at U.S. Ports of Entry 6
Security Vulnerabilities at Unmanned and Unmonitored U.S. Border Locations 10
Corrective Action Briefings and DHS Actions 15

**Appendix I** **Comments from the Department of Homeland Security** 18

**Tables**

Table 1: Entering the United States through Land Ports of Entry 7
Table 2: Entering the United States through Sea and Air Ports of Entry 8
Table 3: Security Vulnerabilities at Unmanned, Unmonitored Locations 11

**Figure**

Figure 1: GAO Investigator Crossing from Canada into the United States in a Northern Border Location 13

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

United States Government Accountability Office
Washington, DC 20548

May 16, 2008

The Honorable Max Baucus
Chairman
The Honorable Charles E. Grassley
Ranking Member
Committee on Finance
United States Senate

Intelligence officials believe that the United States will face a persistent and evolving terrorist threat and that the terrorist group al Qaeda will intensify its efforts to put operatives here. From January 2003 to September 2007, we testified on three occasions before your Committee to describe security vulnerabilities that terrorists could exploit to enter the country.[1] The vulnerabilities are related to traveler screening and border-protection efforts that were consolidated under Customs and Border Protection (CBP), a component of the Department of Homeland Security (DHS), in March 2003. Our first two testimonies were focused on covert testing at ports of entry—the air, sea, and land locations where international travelers can legally enter the United States. For our third testimony, we focused on limited security assessments of unmanned and unmonitored border areas between ports of entry.[2]

This report summarizes the findings of the covert tests and security assessment work performed for your Committee and reported at hearings on January 30, 2003; August 2, 2006; and September 27, 2007. It is important to note that fugitives, smugglers, illegal immigrants, or other criminals could also take advantage of the vulnerabilities we identified. To summarize our work, we reviewed our prior testimonies and the work papers associated with them. We also requested information in writing

[1]See GAO, *Weaknesses in Screening Entrants into the United States*, GAO-03-438T (Washington, D.C.: Jan. 30, 2003); GAO, *Border Security: Continued Weaknesses in Screening Entrants into the United States*, GAO-06-976T (Washington, D.C.: Aug. 2, 2006); and GAO, *Border Security: Security Vulnerabilities at Unmanned and Unmonitored U.S. Border Locations*, GAO-07-884T (Washington, D.C.: Sept. 27, 2007).

[2]Because of safety concerns, we could not perform covert tests at all unmanned and unmonitored border locations. For more information on covert testing, see GAO, *Investigative Operations: Use of Covert Testing to Identify Security Vulnerabilities and Fraud, Waste, and Abuse*, GAO-08-286T (Washington, D.C.: Nov. 14, 2007).

from DHS related to recent efforts to secure U.S. borders and address the vulnerabilities highlighted by our work.

For our testing at ports of entry, we entered the states of Washington, Idaho, Michigan, and New York from Canada; the states of California, Arizona, and Texas from Mexico; the state of Florida from Jamaica; and the state of Virginia from the Bahamas. To create counterfeit documents we used software, hardware, and materials that are available to the public. The tested ports of entry were a nonrepresentative selection we identified using publicly available information. Because we tested a nonrepresentative selection, it is not possible to project the results of our work to any other ports of entry. The unmanned and unmonitored border areas we visited were defined as locations where CBP does not maintain a manned presence 24 hours per day or where there was no apparent monitoring equipment in place. We performed limited security assessments at a nonrepresentative selection of these locations and did not attempt to evaluate all potential U.S. border security vulnerabilities. Where possible, and at your request, investigators attempted to simulate the cross-border movement of radioactive materials or other contraband to highlight the severity of the vulnerability at these border areas. DHS considered some of our results to be law-enforcement sensitive and requested that we not include certain information in our report, such as the names of states we visited for our September 2007 work on unmanned and unmonitored locations.

We prepared this report from January to May 2008. However, all covert tests and security assessment work were performed prior to DHS's January 31, 2008, revised document procedures for U.S. citizens at ports of entry and it is therefore not possible to project our results to these new procedures. We are reporting on the results of testing at land, sea, and air ports of entry; however, the majority of our work was focused on land ports of entry. Further, the results of our covert testing and security assessments are applicable only to U.S. border security efforts and do not relate to efforts made by other governments. Our work was limited in scope and cannot be projected to represent systemic weaknesses in DHS border-protection efforts. Further, it does not address the entry of terrorists into the Bahamas, Canada, Jamaica, or Mexico. As noted in our prior testimonies, we performed all covert testing and security assessment work in accordance with standards prescribed by the President's Council on Integrity and Efficiency.

## Results in Brief

Our investigators identified numerous border security vulnerabilities, both at ports of entry and at unmanned and unmonitored land border locations between the ports of entry. In testing ports of entry, undercover investigators carried counterfeit drivers' licenses, birth certificates, employee identification cards, and other documents, presented themselves at ports of entry and sought admittance to the United States dozens of times. They arrived in rental cars, on foot, by boat, and by airplane. They attempted to enter in four states on the northern border (Washington, New York, Michigan, and Idaho), three states on the southern border (California, Arizona, and Texas), and two other states requiring international air travel (Florida and Virginia). In nearly every case, government inspectors accepted oral assertions and counterfeit identification provided by our investigators as proof of U.S. citizenship and allowed them to enter the country. In total, undercover investigators made 42 crossings with a 93 percent success rate.[3] On several occasions, while entering by foot from Mexico and by boat from Canada, investigators were not even asked to show identification. For example, at one border crossing in Texas in 2006, an undercover investigator attempted to show a CBP officer his counterfeit Virginia driver's license, but the officer said, "That's fine, you can go" without looking at it. As a result of these covert tests, we concluded that terrorists or other criminals could use counterfeit identification to pass freely through most of the tested ports of entry with little chance of being detected.

In our most recent work, we shifted our focus from ports of entry and primarily performed limited security assessments of unmanned and unmonitored areas between ports of entry. The names of the states we visited for this limited security assessment have been withheld at the request of CBP. In four states along the U.S.–Canada border, we found state roads that were very close to the border that CBP did not appear to monitor. In three states, the proximity of the road to the border allowed investigators to cross undetected, successfully simulating the cross-border movement of radioactive materials or other contraband into the United States from Canada. For example, in one apparently unmanned, unmonitored area on the northern border, the U.S. Border Patrol was alerted to our activities through the tip of an alert citizen. However, the

[3]In three cases, our undercover investigators were denied entry into the United States by CBP officers. In the first case, a CBP officer at the Canadian border noticed that our undercover investigator's U.S. passport contained a substituted photo and would not allow him to enter. We believe that the other two cases are linked to this single incident because CBP became aware of our covert testing.

responding U.S. Border Patrol agents were not able to locate the investigators and their simulated contraband. Also on the northern border, investigators located several ports of entry in one state on the northern border that had posted daytime hours and were unmanned overnight. Investigators observed that surveillance equipment was in operation, but that the only preventive measure to stop an individual from crossing the border into the United States was a barrier across the road that could be driven around. We also identified potential security vulnerabilities on federally managed lands adjacent to the U.S.–Mexico border. We concluded that CBP faces significant challenges on the northern border, and that a determined cross-border violator would likely be able to bring radioactive materials or other contraband undetected into the United States by crossing the U.S.–Canada border at any of the assessed locations. A brief video highlighting the vulnerabilities we found during this investigation is available on the Internet at: http://www.gao.gov/media/video/gao-07-884t/.

We held corrective action briefings with CBP in 2006 and 2007 to discuss the results of our prior work. CBP generally agreed with our August 2006 findings and acknowledged that its officers are not able to identify all forms of counterfeit identification presented at land border crossings. In addition, in response to our August 2006 work, CBP officials stated that they supported the Western Hemisphere Travel Initiative[4] and were working to implement it. This initiative has several parts, the most recent of which went into effect on January 31, 2008. In response to our September 2007 report, CBP indicated that resource restrictions prevent U.S. Border Patrol agents from investigating all instances of suspicious activity. For example, in the September 2007 hearing on border security before your Committee, a CBP official stated that roughly 250 U.S. Border Patrol agents were patrolling the U.S.–Canada border at any given time. This represents a quarter of all agents reportedly assigned to patrol the northern border during that period because the agents work in shifts, and may not be on duty due to sick leave or vacation time. CBP stated that the northern border presents more of a challenge than the southern border for several reasons, including the wide expanse of the border and the existence of many antiquated ports of entry.

[4]DHS and the Department of State's effort to specify acceptable documents and implement document requirements at 326 air, land, and sea ports of entry is called the Western Hemisphere Travel Initiative.

In response to this report, DHS provided a written update on numerous border protection efforts it has taken to enhance border security since 2003. We did not attempt to verify the information provided by DHS, but have included the response in appendix I.

## Background

CBP is the lead federal agency in charge of securing the nation's borders. When CBP was created, it represented a merger of components from three agencies—the U.S. Customs Service, the U.S. Immigration and Naturalization Service (INS), and the Animal and Plant Health Inspection Service. Under the Immigration and Nationality Act, its implementing regulations, and CBP policies and procedures, CBP officers are required to establish, at a minimum, the nationality of individuals and whether they are eligible to enter the country at ports of entry. All international travelers attempting to enter the country through ports of entry undergo primary inspection, which is a preliminary screening procedure to identify those legitimate international travelers who can readily be identified as admissible.

Regarding land ports of entry, the United States shares over 5,000 miles of border with Canada to the north (including the state of Alaska), and 1,900 miles of border with Mexico to the south. Individuals attempting to legally enter the United States by land present themselves to a CBP officer at one of the 170 ports of entry located along these borders. During the period of our investigations, U.S. citizens could gain entry to the United States by establishing their citizenship to the satisfaction of U.S. officials at a land port of entry. While this frequently involved a citizen presenting their birth certificate, photo identification (e.g., a driver's license), or baptismal records, the law did not require U.S. citizens to present any of these documents as proof of citizenship. Until recently, U.S. citizens could enter the country at land ports of entry based only on oral statements. However, as of January 31, 2008, U.S. citizens age 19 and older are required, under the Western Hemisphere Travel Initiative, to present both proof of identity and citizenship when attempting to enter the United States by land. Documents that would fulfill this requirement could include a passport, a military ID with travel orders, or an enhanced driver's license. In the absence of a single document that establishes both proof of identity and citizenship, U.S. citizens require multiple documents, such as a driver's license and a birth certificate, to enter the United States. Requirements for entering the United States by sea are similar to those for entering by land. Regarding air ports of entry, starting on January 23, 2007, U.S. citizens were required, under the Western Hemisphere Travel Initiative, to present

a passport or secure travel document when entering the United States. Prior to the implementation of this initiative, U.S. citizens entering the country by air from such locations as the Bahamas, Mexico, and Jamaica could establish their citizenship by oral assertions and documents such as drivers' licenses and birth certificates.

It is illegal to enter the United States at any location other than a port of entry. The U.S. Border Patrol, a component of CBP, patrols and monitors areas between ports of entry. However, given limited resources and the wide expanse of the border, the U.S. Border Patrol is limited in its ability to monitor the border either through use of technology or with a consistent manned presence. Commensurate with its perception of the threat, CBP has distributed human resources differently on the northern border than it has on the southern border. According to CBP, as of May 2007, it had 972 U.S. Border Patrol agents assigned to the northern border and 11,986 agents assigned to the southern border. The number of agents actually providing border protection at any given time is far smaller than these figures suggest. As mentioned above, in the September 2007 hearing on border security before your Committee, a CBP official stated that roughly 250 U.S. Border Patrol agents were patrolling the U.S.–Canada border at any given time—about a quarter of all agents reportedly assigned to patrol the northern border during that period.

## Security Vulnerabilities at U.S. Ports of Entry

We found two types of security vulnerabilities in our covert testing at ports of entry. First, we found that, in the majority of cases, the government inspectors who reviewed our undercover investigators' counterfeit documentation did not know that they were bogus and allowed them to enter the country. Second, we found that government officials did not always ask for identification. Although it was not a requirement for government officials to ask for identification at the time we performed our tests, we concluded that this was a major vulnerability that could allow terrorists or other criminals to easily enter the country.

In table 1 below, each individual instance of an investigator crossing the border is noted separately, although, in some cases, investigators crossed the border in groups of two or more.

**Table 1: Entering the United States through Land Ports of Entry**

| No. | Date | Country of departure | Documents provided | Result |
|---|---|---|---|---|
| 1 | November 2002 | Mexico | No documents provided | Passed |
| 2 | November 2002 | Mexico | Counterfeit driver's license | Passed |
| 3 | November 2002 | Mexico | Counterfeit driver's license | Passed |
| 4 | December 2002 | Canada | Counterfeit driver's license and birth certificate | Passed |
| 5 | December 2002 | Canada | Counterfeit driver's license | Passed |
| 6 | August 2003 | Canada | Counterfeit driver's license | Passed |
| 7 | August 2003 | Canada | Counterfeit driver's license | Passed |
| 8 | October 2003 | Canada | Counterfeit driver's license and employee ID | Passed |
| 9 | October 2003 | Canada | Counterfeit U.S. passport and driver's license | Denied entry |
| 10 | November 2003 | Mexico | Counterfeit driver's license | Passed |
| 11 | November 2003 | Mexico | Counterfeit U.S. passport | Passed |
| 12 | December 2003 | Mexico | Counterfeit driver's license | Passed |
| 13 | December 2003 | Mexico | Counterfeit U.S. passport | Passed |
| 14 | February 2006 | Mexico | Counterfeit driver's license | Passed |
| 15 | February 2006 | Mexico | Counterfeit driver's license | Passed |
| 16 | February 2006 | Mexico | No documents provided | Passed |
| 17 | February 2006 | Mexico | Counterfeit driver's license | Passed |
| 18 | March 2006 | Mexico | Counterfeit driver's license | Passed |
| 19 | March 2006 | Mexico | Counterfeit driver's license | Passed |
| 20 | March 2006 | Mexico | No documents provided | Passed |
| 21 | March 2006 | Mexico | No documents provided | Passed |
| 22 | May 2006 | Canada | Counterfeit driver's license and birth certificate | Passed |
| 23 | May 2006 | Canada | Counterfeit driver's license and birth certificate | Passed |
| 24 | May 2006 | Canada | Counterfeit driver's license | Passed |
| 25 | May 2006 | Canada | Counterfeit driver's license | Passed |
| 26 | May 2006 | Canada | Counterfeit driver's license | Passed |
| 27 | May 2006 | Canada | Counterfeit driver's license | Passed |
| 28 | May 2006 | Canada | Counterfeit driver's license and birth certificate | Passed |
| 29 | May 2006 | Canada | Counterfeit driver's license and birth certificate | Passed |
| 30 | May 2006 | Canada | Counterfeit driver's license | Passed |
| 31 | May 2006 | Canada | Counterfeit driver's license | Passed |

Source: GAO.

Note: DHS considered the consolidated listing of destination states to be law enforcement sensitive information. Therefore, this table does not include the names of the states investigators entered.

We consider our attempts to enter the country through sea and air ports of entry as different from our land crossings. For one thing, we did not perform the same amount of testing that we performed at land ports of entry. For another, the standard for admittance via air ports of entry continues to be stricter than via land and sea routes. In table 2 below, each individual instance of an investigator entering the United States via air or sea is noted separately.

**Table 2: Entering the United States through Sea and Air Ports of Entry**

| No. | Date | Country of departure | Port type | Documents provided | Result |
|---|---|---|---|---|---|
| 1 | September 2002 | Canada | Sea | No documents provided | Passed |
| 2 | September 2002 | Canada | Sea | No documents provided | Passed |
| 3 | January 2003 | Jamaica | Air | Counterfeit driver's license and birth certificate | Passed |
| 4 | January 2003 | Jamaica | Air | Counterfeit driver's license and birth certificate | Passed |
| 5 | August 2003 | Canada | Sea | Counterfeit driver's license and birth certificate | Passed |
| 6 | August 2003 | Canada | Sea | Counterfeit driver's license and birth certificate | Passed |
| 7 | January 2004 | Jamaica | Air | Counterfeit U.S. passport and driver's license | Denied entry |
| 8 | January 2004 | Jamaica | Air | Counterfeit driver's license and birth certificate | Denied entry |
| 9 | March 2004 | Bahamas | Air | Counterfeit driver's license and birth certificate | Passed |
| 10 | March 2004 | Bahamas | Air | Counterfeit driver's license and birth certificate | Passed |
| 11 | March 2004 | Bahamas | Air | Counterfeit driver's license and birth certificate | Passed |

Source: GAO.

Note: DHS considered the consolidated listing of destination states to be law enforcement sensitive information. Therefore, this table does not include the names of the states investigators entered.

Selected details related to these covert tests are discussed below.

## Counterfeit Identification Accepted as Proof of Citizenship in Most Cases

For our 2003 testimony, investigators successfully entered the United States using counterfeit drivers' licenses and other bogus documentation through a land port of entry in Washington. They also entered Florida via air from Jamaica using the same counterfeit documentation. Similar follow-up work was performed throughout 2003 and 2004, resulting in successful entry at locations in Washington, New York, California, Texas, and Virginia using counterfeit identification. In 2006, investigators successfully entered the United States using counterfeit drivers' licenses and other bogus documentation through seven land ports of entry on the northern and southern borders, adding the states of Michigan, Idaho, and Arizona to the list of states they had entered.

In the majority of cases, investigators entered the country by land using rental cars. When requested, they displayed counterfeit Virginia and West Virginia drivers' licenses and birth certificates to the government officials at ports of entry. They also used bogus U.S. passports and, in one case, a fake employee identification card in the name of a major U.S. airline. Government officials typically inspected the documentation while inquiring whether our undercover investigators were U.S. citizens. On some occasions, the officials asked whether our investigators had purchased anything in Canada or Mexico. In several instances, CBP officials asked our investigators to leave their vehicles and inspected the vehicles; they appeared to be searching for evidence of smuggling. In only one case on the northern border, one of our undercover investigators was denied entry because a CBP officer became suspicious of the expired U.S. passport with substituted photo offered as proof of citizenship.[5]

## Undercover Investigators Did Not Show Identification in All Cases

For our 2003 testimony, we found that INS inspectors did not request identification at a sea port of entry in Washington and a land port of entry in California. Our investigators' oral assertions that they were U.S. citizens satisfied the INS inspectors and they were allowed to enter the country. Later, while conducting our 2006 covert tests, we found that CBP officers did not request identification during several foot crossings from Mexico. For example, on February 23, 2006, two investigators crossed the border from Mexico into Texas on foot. When the first investigator arrived at the port of entry, he was waved through without being asked to show identification. At this point, the investigator asked the CBP officer whether he wished to see any identification. The officer replied, "OK, that would be good." The investigator began to remove his counterfeit Virginia driver's license from his wallet when the officer said "That's fine, you can go." The CBP officer never looked at the license. However, the CBP officer did request identification from the investigator who was walking behind the first investigator.

In another test on March 15, 2006, two investigators entered Arizona from Mexico by foot. They had received a phone call in advance from another investigator who had crossed the border earlier using genuine identification. He said that the CBP officers on duty had swiped his

[5]As a result of this incident, we believe CBP became aware of our covert testing and denied entry to two undercover investigators when they attempted to enter the country from Jamaica. Investigators were admitted to the United States after revealing they were GAO employees and providing real identification.

driver's license through a scanning machine. Because the counterfeit drivers' licenses the other two investigators were carrying had fake magnetic strips, the investigators realized they could be questioned by CBP officers if their identification cards did not scan properly. When the two investigators arrived at the port of entry, they engaged one of the officers in conversation to distract him from scanning their drivers' licenses. After a few moments, the CBP officer asked the investigators if they were both U.S. citizens. They said, "yes." He then asked the investigators if they had purchased anything in Mexico, and they responded, "no." The CBP officer then said, "Have a nice day" and allowed them to enter the United States. He did not ask for any identification.

## Security Vulnerabilities at Unmanned and Unmonitored U.S. Border Locations

We first reported on potential security vulnerabilities at unmanned and unmonitored border areas in our 2003 testimony. While conducting testing at U.S.–Canada ports of entry, we found that one of our investigators was able to walk into the United States from Canada at a park straddling the border. The investigator was not stopped or questioned by law enforcement personnel from either Canada or the United States. In our September 2007 testimony, we reported on similar vulnerabilities at unmanned and unmonitored locations on the northern and southern borders. The unmanned and unmonitored border areas we visited were defined as locations where CBP does not maintain a manned presence 24 hours per day or where there was no apparent monitoring equipment in place. Safety considerations prevented our investigators from performing the same assessment work on the U.S.–Mexico border as performed on the northern border.

We found three main vulnerabilities during this limited security assessment. First, we found state roads close to the border that appeared to be unmanned and unmonitored, allowing us to simulate the cross-border movement of radioactive materials or other contraband from Canada into the United States. Second, we also located several ports of entry that had posted daytime hours and which, although monitored, were unmanned overnight. Investigators observed that surveillance equipment was in operation but that the only observable preventive measure to stop a cross-border violator from entering the United States was a barrier across the road that could be driven around. Finally, investigators identified potential security vulnerabilities on federally managed lands adjacent to the U.S.–Mexico border. These areas did not appear to be monitored or have a noticeable law enforcement presence during the time our investigators visited the sites. See table 3 for a summary of the vulnerabilities we found and the activity of investigators at each location.

**Table 3: Security Vulnerabilities at Unmanned, Unmonitored Locations**

| Security vulnerability | Location | Investigator activity | Law enforcement response and additional observations |
|---|---|---|---|
| State roads close to the border | 1 | Simulated the cross-border movement of radioactive materials or other contraband into the United States from Canada | • No visible law enforcement response<br>• No observable electronic monitoring equipment<br>• Suspicious activity was reported to the U.S. Border Patrol, but responding agents were unable to locate investigators and their simulated contraband |
| | 2 | Took photographs of over half a dozen locations where state roads ended at the U.S.–Canada border | • No visible law enforcement response despite suspicious activity<br>• No observable electronic monitoring equipment<br>• CBP stated that our activities would not be grounds for a formal investigation |
| | 3 | Simulated the cross-border movement of radioactive materials or other contraband into the United States from Canada | • No visible law enforcement response<br>• No observable electronic monitoring equipment |
| | 4 | Simulated the cross-border movement of radioactive materials or other contraband into the United States from Canada | • Some surveillance cameras and law enforcement presence noted along the road<br>• Investigators crossed the border into the United States in a spot that appeared to be unmanned and unmonitored, then returned to Canada |
| | 5 | Approached the U.S.–Mexico border | • Large law enforcement effort at this location, including U.S. Army National Guard units and unmanned aerial vehicles<br>• Investigator approached the border in a spot that appeared to be unmanned and unmonitored<br>• According to CBP, because our investigators did not approach from the direction of Mexico, there would be no expectation for law enforcement units to question these activities |
| Ports of entry with posted hours | 6 | Attempted to trigger a law enforcement response by taking photographs of a port of entry that had closed for the night | • A gate was placed across the road, but investigators observed it would be possible to drive around the gate<br>• U.S. Border Patrol responded 20 minutes after investigators were caught on camera at the port of entry<br>• Responding U.S. Border Patrol agent did not attempt to verify identity of investigators or search their vehicle |
| Federally managed lands adjacent to border | 7 | Approached the U.S.–Mexico border | • No visible law enforcement response<br>• No observable electronic monitoring equipment<br>• Investigators observed evidence of frequent border crossings into the United States at this location |
| | 8 | Stepped over a 4-foot-high border fence, entered Mexico, and returned again to the United States | • No visible law enforcement response<br>• No observable electronic monitoring equipment<br>• No observed law enforcement presence despite proximity to border |

Source: GAO.

Selected details related to these covert tests are discussed below.

## State Roads Close to the Border

According to CBP, the ease and speed with which a cross-border violator can travel to the border, cross the border, and leave the location of the crossing are critical factors in determining whether an area of the border is vulnerable. We identified state roads close to the border that appeared to be unmanned and unmonitored, allowing us to simulate the cross-border movement of radioactive materials or other contraband from Canada into the United States. For example, on October 31, 2006, our investigators positioned themselves on opposite sides of the U.S.–Canada border in an unmanned location. Our investigators selected this location because roads on either side of the border would allow them to quickly and easily exchange simulated contraband. After receiving a signal by cell phone, the investigator in Canada left his vehicle and walked approximately 25 feet to the border carrying a red duffel bag. While investigators on the U.S. side took photographs and made a digital video recording, the individual with the duffel bag proceeded the remaining 50 feet, transferred the duffel bag to the investigators on the U.S. side, and returned to his vehicle on the Canadian side. The set up and exchange lasted approximately 10 minutes, during which time the investigators were in view of residents both on the Canadian and U.S. sides of the border. According to CBP records of this incident, an alert citizen notified the U.S. Border Patrol about the suspicious activities of our investigators. The U.S. Border Patrol subsequently attempted to search for a vehicle matching the description of the rental vehicle our investigators used. However, the U.S. Border Patrol was not able to locate the investigators with the duffel bag, even though they had parked nearby to observe traffic passing through the port of entry.

See figure 1 for a photograph of our investigator crossing the northern border at another unmanned, unmonitored location on the northern border with simulated contraband.

**Figure 1: GAO Investigator Crossing from Canada into the United States in a Northern Border Location**

Source: GAO.

Note: Investigator's face has been blurred to protect his identity.

In contrast to our observations on the northern border, our investigators observed a large law enforcement and Army National Guard presence near a state road on the southern border, including unmanned aerial vehicles. On October 17, 2006, two of our investigators left a main U.S. route about a quarter mile from a U.S.–Mexico port of entry. Traveling on a dirt road that parallels the border, our investigators used a GPS system to get as close to the border as possible. Our investigators passed U.S. Border Patrol agents and U.S. Army National Guard units. In addition, our investigators spotted unmanned aerial vehicles and a helicopter flying parallel to the border. At the point where the dirt road ran closest to the U.S.–Mexico border, our investigators spotted additional U.S. Border Patrol vehicles parked in a covered position. About three-fourths of a mile from these vehicles, our investigators pulled off the road. One investigator exited the vehicle and proceeded on foot through several gulches and gullies toward the Mexican border. His intent was to find out whether he would be questioned by law enforcement agents about his activities. He returned to the vehicle after 15 minutes, at which time our investigators returned to the main road. Our investigators did not observe any public traffic on this road for the 1 hour

that they were in the area, but none of the law enforcement units attempted to stop our investigators and find out what they were doing. According to CBP, because our investigators did not approach from the direction of Mexico, there would be no expectation for law enforcement units to question these activities.

## Ports of Entry with Posted Hours

We also identified several ports of entry with posted daytime hours in one state on the northern border. During the daytime these ports of entry are staffed by CBP officers. During the night, CBP told us that it relies on surveillance systems to monitor, respond to, and attempt to interdict illegal border crossing activity. For example, on November 14, 2006, at about 11:00 p.m., our investigators arrived on the U.S. side of one port of entry that had closed for the night. Investigators observed that surveillance equipment was in operation but that the only visible preventive measure to stop an individual from entering the United States was a barrier across the road that could be driven around. CBP provided us with records that confirmed our observations about the barrier at this port of entry, indicating that on one occasion a cross-border violator drove around this type of barrier to illegally enter the United States. Although the violator was later caught by state law enforcement officers and arrested by the U.S. Border Patrol, we were concerned that these ports of entry were unmanned overnight.

## Federally Managed Lands

Investigators identified potential security vulnerabilities on federally managed land adjacent to the U.S.–Mexico border. These areas did not appear to be monitored or have a manned CBP presence during the time our investigators visited the sites. For example, on January 9, 2007, our investigators entered federally managed land adjacent to the U.S.–Mexico border. The investigators had identified a road running parallel to the border in this area. Our investigators were informed by an employee of a visitor center that because the U.S. government was building a fence, the road was closed to the public. However, our investigators proceeded to the road and found that it was not physically closed. While driving west along this road, our investigators did not observe any surveillance cameras or law enforcement vehicles. A 4-foot-high fence (appropriate to prevent the movement of a vehicle rather than a person) stood at the location of the border. Our investigators pulled over to the side of the road at one location. To determine whether he would activate any intrusion alarm systems, one investigator stepped over the fence, entered Mexico, and returned to the United States. The investigators remained in the location

for approximately 15 minutes but there was no observed law enforcement response to their activities.

In another example, on January 23, 2007, our investigators arrived on federally managed lands adjacent to the U.S.–Mexico border. In this area, the Rio Grande River forms the southern border between the United States and Mexico. After driving off-road in a 4x4 vehicle to the banks of the Rio Grande, our investigators observed, in two locations, evidence that frequent border crossings took place. In one location, the investigators observed well-worn footpaths and tire tracks on the Mexican side of the river. At another location, a boat ramp on the U.S. side of the Rio Grande was mirrored by a boat ramp on the Mexican side. Access to the boat ramp on the Mexican side of the border had well-worn footpaths and vehicle tracks. An individual who worked in this area told our investigators that at several times during the year, the water is so low that the river can easily be crossed on foot. Our investigators were in this area for 1 hour and 30 minutes and observed no surveillance equipment, intrusion alarm systems, or law enforcement presence. Our investigators were not challenged regarding their activities.

After performing our limited security assessment of these locations, investigators learned that a memorandum of understanding exists between DHS (of which CBP is a component), the Department of the Interior, and the Department of Agriculture regarding the protection of federal lands adjacent to U.S. borders. Although CBP is ultimately responsible for protecting these areas, officials told us that certain legal, environmental, and cultural considerations limit options for enforcement—for example, environmental restrictions and tribal sovereignty rights.

## Corrective Action Briefings and DHS Actions

We held corrective action briefings with CBP in 2006 and 2007 to discuss the results of our prior work. CBP generally agreed with our August 2006 findings and acknowledged that its officers are not able to identify all forms of counterfeit identification presented at land border crossings. In addition, in response to our August 2006 work, CBP officials stated that they supported the Western Hemisphere Travel Initiative and were working to implement it. This initiative has several parts, the most recent of which went into effect on January 31, 2008. In response to our September 2007 report, CBP indicated that resource restrictions prevent U.S. Border Patrol agents from investigating all instances of suspicious activity. CBP stated that the northern border presents more of a challenge

than the southern border for several reasons, including the wide expanse of the border and the existence of many antiquated ports of entry.

In response to this report, DHS provided a written update on numerous border protection efforts it has taken to enhance border security since 2003. To directly address vulnerabilities related to bogus documentation, DHS stated that measures have been implemented to enhance CBP officers' ability to detect fraudulent documents, such as

- providing updated fraudulent document training modules to the CBP Academy for inclusion in its curriculum,
- implementing mandatory refresher training in detecting fraudulent documents, and
- providing the 11 ports of entry that have the highest rate of fraudulent document interceptions with advanced equipment to assist with the examination and detection of fraudulent documents.

DHS also pointed out that, effective January 31, 2008, it has ended verbal declarations of citizenship at border crossings and now requires documents for U.S. citizens. If implemented effectively, this would address some of the vulnerabilities we identified in our 2003 and 2006 testimonies. According to DHS, although the full implementation of its Western Hemisphere Travel Initiative has been delayed, the implementation will also address vulnerabilities cited in our testimonies.

In addition, DHS indicated that it has taken a number of actions related to the security of the northern border. In particular, DHS states that, as of April 2008, there were 1,128 agents assigned to the Northern Border—a 16 percent increase from the 972 agents identified in our 2007 report. Furthermore, DHS plans to double personnel staffing levels over the next 2 years to over 2,000 agents by the end of fiscal year 2010. DHS also indicates that CBP has established a field testing division to perform covert tests that appear similar to our own tests, with a particular focus on detecting and preventing illicit radioactive material from entering the United States. We addressed DHS technical and sensitivity comments as appropriate. We did not attempt to verify the information provided by DHS, but have included its full response in appendix I.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we will plan no further distribution until 30 days from

the report date. At that time, we will provide copies of this report to the Secretary of Homeland Security and interested congressional committees and members. We will also make copies available to others upon request. In addition, this report will be available at no charge on the GAO Web site at http://gao.gov.

Please contact me at (202) 512-6722 or kutzg@gao.gov if you or your staffs have any questions concerning this report. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report included John Cooney, Assistant Director; Andy O'Connell, Assistant Director; Barbara Lewis, Andrew McIntosh, Sandra Moore, and Barry Shillito.

Gregory D. Kutz, Managing Director
Forensic Audits and Special Investigations

# Appendix I: Comments from the Department of Homeland Security

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

US GAO

2008 MAY -2 PM 12: 49

May 1, 2008

Mr. Gregory D. Kutz
Managing Director, Forensic Audits &
Special Investigations
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Kutz:

Re: Draft Report GAO-08-757, Border Security: Summary of Covert Tests and Security Assessments for the Senate Committee on Finance for 2003-2007 (Job Code 192271)

Thank you for the opportunity to review and comment on the draft report. United States Customs and Border Protection (CBP) officials provided the following updates.

The report summarizes findings of the GAO's covert tests and security assessment work performed and reported at hearings from 2003 through 2007. U.S. Customs and Border Protection's Office of Internal Affairs conducts covert and overt testing of CBP operations through its Operational Field Testing Division (OFTD). The division was established to test and evaluate CBP's capabilities to detect and prevent illicit radioactive material from entering the United States. The test protocols focused on identifying potential technological vulnerabilities and/or systemic procedural and policy weaknesses related to the screening and detection of passengers and containers entering the United States with illicit radioactive material.

As of April 23, 2008, OFTD reported that they successfully tested and evaluated two CBP land border crossings on their capabilities to detect and prevent terrorists and illicit radioactive material from entering the United States. In addition, consistent with the *Security and Accountability for Every (SAFE) Port Act of 2006*, OFTD covertly and overtly tested and evaluated 21 of the Nation's top 22 busiest seaports for radiation detection and the effectiveness of the non-intrusive imaging radiation equipment deployed at the seaports.

Overall, it was noted that the test results underscored the effectiveness of the radiation detection technology and the CBP officers' compliance with national and local radiation detection response protocols while calling attention to areas for improvement.

www.dhs.gov

The OFTD also developed a testing protocol that will assess and evaluate the CBP officers' capabilities to detect and prevent terrorists and travelers using fraudulent travel documents from entering the United States. The OFTD anticipates these tests will commence before the end of the fiscal year.

The GAO report also focused on reported vulnerabilities on the northern and southern borders. CBP believes that the right combination of personnel, technology, tactical infrastructure and intelligence/partnerships are being deployed to address southern and northern border vulnerabilities.

On the northern border, CBP has deployed additional Border Patrol agents from the southwest border to the northern border with 1,800 expected by September 2009. In addition, CBP conducts joint operations with the Department of Defense's Joint Task Force – North, continues to pilot maritime technology projects incorporating ground based radar and proof of concept multi-sensor systems, and seeks increased liaisons with our Canadian partners through Project North Star and the Integrated Border Enforcement Teams. CBP also is expanding Air and Marine operations on the northern border, including the deployment of Predator B Unmanned Aircraft Systems.

On the southern border, CBP is developing SBI*net,* a Department of Homeland Security (DHS) program that will provide Border Patrol the appropriate mixture of personnel, technology, and infrastructure, combined into a common operational picture for the purpose of securing both the northern and southern borders. SBI*net* personnel are charged with designing, developing, and implementing a solution that incorporates surveillance and detection, command and control, intelligence, tactical infrastructure, communications and information technology. SBI*net* will use the latest innovative technology – cameras, biometrics, sensors, air assets, improved communications systems – to provide Border Patrol agents what they need to execute the agency's mission in the safest and most effective manner. Moving forward, CBP intends to complete construction on the 370 miles of pedestrian fencing and 300 miles of vehicle fencing along the southern border to enhance border security. Currently CBP has almost 170 miles of primary pedestrian fencing and 135 miles of vehicle fence in place.[1] Plans are to complete construction of the full 670 miles of fencing by the end of the calendar year.

CBP completed technology requirements assessments of the Yuma, Tucson, and El Paso sectors and will look to fill those needs first as they present the highest threat areas. CBP currently has 4 mobile surveillance systems in operation and plans to deploy additional systems this year to the southwest border to serve as primary detection platforms. CBP also deployed over 7,500 unattended ground sensors (UGS) that provide continuous, low-cost, and covert awareness of cross-border activity. CBP is acquiring 2,500 additional UGS this fiscal

[1] Figures for miles of pedestrian fencing and vehicle fencing in place include those miles that have been constructed since October 2007, toward the achievement of the calendar year 2008 goal of deploying an additional 225 miles of pedestrian fencing and 185 miles of vehicle fencing along the southwest border. When these goals are achieved, CBP will have a total of 370 miles of pedestrian fencing and 300 miles of vehicle fencing.

2

year with 1,250 of those planned for deployment on the northern border and 1,250 on the southwest border.

Dovetailing with the efforts on the southern border, Congress directed CBP to redirect $20 million of the Border Security, Fencing, Infrastructure, and Technology appropriation "to begin addressing needs and vulnerabilities along the northern border." Accordingly, CBP is developing a SBI*net* prototype that will inform and demonstrate the technology issues associated with the integration of air, land and maritime assets into a common operating picture on the northern border.

Referring to both borders, the GAO report indicated that the GAO found two types of security vulnerabilities in their covert testing at ports of entry. The first vulnerability cited by the GAO is that some of the counterfeit documents presented by their undercover investigators went undetected by CBP officers. In an effort to enhance fraudulent document training, CBP inserted updated training into the CBP Academy curriculum as well as implemented mandatory refresher training on detecting fraudulent documents. In addition, CBP provided the ports of entry that have the highest rate of fraudulent document interceptions with advanced equipment to assist with the examination and detection of fraudulent documents.

The second vulnerability cited by GAO in this report is that investigators were not asked to provide identification.[2] The GAO acknowledged that asking for identification was not a requirement at the time of the covert test however they concluded that "this was a major vulnerability that could allow terrorists or other criminals to easily enter the country." The full implementation of the Western Hemisphere Travel Initiative (WHTI) will address this and other vulnerabilities; however, the Congress has delayed its completion. In the interim, DHS is exercising its preexisting authority to require appropriate government documents at the border and end verbal declarations of citizenship. It is important to clarify that the implementation of WHTI is separate from the ending of verbal declarations. While they both work to enhance border security they are not interchangeable initiatives as the GAO report reflects.

Effective January 31, 2008, under the aforementioned authority, United States, Canadian and Bermudian citizens are required to present one or more government-issued documents to prove identity and citizenship. Children ages 18 and under need only present a birth certificate. This transition inhibits entry of individuals who cannot confirm their identity and citizenship. Since the transition, changes in travel document requirement have not caused discernable increases in wait times at the border. Compliance rates are high and continue to

[2] The GAO report implies that the failure of CBP officers and agents to approach GAO investigators while inside the United States represents a security vulnerability. However, GAO acknowledges that Border Patrol agents and unmanned aerial vehicles were observed monitoring the border during the October 2006 GAO investigation on the southern border. GAO presents no evidence that investigators were not being monitored appropriately by CBP during the entire time that investigators were along the U.S./Mexico border. The report does not address the likely possibility that Border Patrol agents would have approached the investigators while on foot or in their vehicle as appropriate if there was a suspicion of unlawful activity.

3

increase. United States and Canadian citizens are presenting the requested documents when crossing the border.

High compliance rates have also been reported during the initial phase of the WHTI. As of January 23, 2007, the WHTI Air Final Rule requires all arriving air travelers, regardless of age, to present a passport or other acceptable secure document for entry into the United States. In the last seven months, CBP has reported a compliance rate of 99 percent for citizens of the United States, Canada, and Bermuda, and there has been no interruption to air transportation. This is the result of close coordination with federal government partners, private sector travel, tourism industry and the air carriers. The high level of compliance shows that Americans and foreign nationals alike are willing and able to obtain the necessary documents to enter or re-enter the United States once the requirements are known and enforced. On March 27, 2008, DHS announced that full implementation of the land and sea provisions of WHTI would begin July 1, 2009.

As reflected in the report, CBP officials are tasked with a very complex, dangerous, and challenging job. They face those challenges every day with vigilance, dedication to service, and integrity as they work to strengthen national homeland security and protect America and its citizens.

Attachment I "Recent and Planned Border Security Initiatives" provides additional, detailed information on Department activities.

Technical and sensitivity comments have been provided under separate cover. We request that the GAO make appropriate changes in the draft report prior to releasing information that has been determined to be sensitive. We expect GAO to accord this material the same level of sensitivity as DHS. Any further disclosure only should occur with the express permission of the Department.

Sincerely,

Penelope G. McCormack
Acting Director
Departmental GAO/OIG Liaison Office

4

Attachment I

**Recent and Planned Border Security Activities**

**Northern Border Overview**

**Personnel**

Border Patrol agent staffing on the Northern Border has increased significantly since September 11, 2001. Prior to 9-11, there were only 340 Border Patrol agents assigned to the Northern Border responsible for securing nearly 4,000 miles of international border with Canada. As of April 2008, there were 1,128 agents assigned to the Northern Border, a 16 percent increase from the 972 agents identified in the 2007 GAO report. Furthermore, personnel staffing levels will be doubled over the next two years to over 2,000 agents by the end of Fiscal Year 2010. These additional agents will be deployed to traditional assignments such as line watch but will also be assigned to liaison duties in the following offices:

- Integrated Border Enforcement Teams
  - Border Enforcement and Security Teams (BEST) pilot locations
- Intelligence and Operations Coordination Centers
- US Attorney's Offices
- Royal Canadian Mounted Police (RCMP)
- State Fusion Centers
- Local Task Forces

**Technology**

The apparent lack of visibility of Border Patrol resources does not mean that the border is "unmanned and unmonitored." The Border Patrol currently employs a myriad of tactics to enforce border security along the Northern Border. These include but are not limited to ground surveillance sensors and cameras. Future technology includes:

- Three-Ground Surveillance Radars will be deployed along the Northern Border.
- The total number of unattended ground sensors deployed will increase and existing unattended ground sensors will be replaced with upgraded sensors and strategically deployed along the Northern Border in FY 2008.
  - The RCMP has deployed ground sensors in strategic locations in coordination with the US Border Patrol.
- Improved mobile Infra-Red detection capability is being deployed to every Northern Border Sector.

5

- The existing Remote Video Surveillance System in the Blaine Washington Sector will be upgraded to provide enhanced coverage of the border.

- The deployment of interim technology will continue in the form of thermal night vision devices and G-2 Sentinel Systems which are advanced game cameras with video/unattended ground sensor capabilities.

- SBInet Northern Demonstration Project: The demonstration will take place along the Lower St. Clair River in the Detroit Sector Area of Responsibility (AOR). The prototype will demonstrate how an integrated air, land and maritime border security solution will improve operations in an area of the Northern Border; improve situational awareness by integrating national and tactical intelligence sources into a common operating picture; and provide members of the border enforcement community with the information necessary to support homeland security strategies and plans for unity of effort.

- Additional DHS Science and Technology and CBP Office of Information Technology pilot projects will be tested throughout the northern border. These pilot projects will involve four sectors and include the:

    - Use of bollards in the Blaine sector;
    - Placement of acoustic sensors in the Spokane sector to detect low flying aircraft incursions;
    - Testing of gel-celled unattended ground sensors in the Grand Forks sector; and
    - BorderNet proof-of-concept pilot program in the Swanton sector which is designed to enhance current and future detection capabilities in a Northern Border operational environment.

**Partnerships**

Liaison and intelligence sharing have been improved and increased with Federal, State and local law enforcement agencies, as well as with counterparts within the Canadian government.

- Integrated Border Enforcement Teams (IBETS)
    - The IBETs are bi-national, multi-agency law enforcement teams that enhance border integrity and security by identifying, investigating, and interdicting persons and organizations that pose a threat to national security or are engaged in other organized criminal activity.

- Border Enforcement and Security Teams
    - Two Immigration and Customs Enforcement BEST pilots will begin in the Buffalo and Blaine Sectors. These teams will provide investigative support to IBETS.

6

- Royal Canadian Mounted Police
  - An RCMP Inspector has been detailed to the Border Patrol Headquarters to serve as a liaison between the two agencies.
  - Border Patrol is seeking to embed agents into the RCMP Divisions to enhance the dissemination of actionable intelligence and to ensure optimum information sharing with our Canadian partners.

- Project North Star
  - A bi-national forum that provides Canadian and U.S. law enforcement managers a mechanism to enhance existing communications, cooperation, and partnership between agencies and personnel that operate within the border area.

- Northern Border Intelligence and Operations Coordination Centers (IOCC)
  - Multi-Component Intelligence Fusion Centers that facilitate the communication, intelligence and flow of information throughout a specific region to multiple law enforcement agencies.

- Airfields Initiative
  - The development of strong partnerships and liaison with the community and law enforcement organizations to gather and develop intelligence information on aircraft incursions.

- Radio Interoperability Pilot Project
  - Havre Border Patrol Sector and RCMP are participating in a pilot program that uses techniques to measure interoperability of radio systems.

**Southern Border Updates**

**Personnel**

Based on the operational needs of the Border Patrol, for Fiscal Year 2008, staffing will increase between 18 to 20 percent along the Southern border. As of April 2008, there were 14,138 agents assigned to the Southern border. That represents an increase of 18 percent from the 11,986 agents identified in the 2007 GAO report.

**Technology**

The Border Patrol is working towards the deployment of technology across the Southwest Border in an effort to gain operational control of our nation's border.

- Ongoing delivery of 40 Mobile Surveillance Systems units to the southern border is occurring.

7

- TUSCON-1 deployment: Will consist of the construction and placement of sensor and communication towers in the Tucson Station area of responsibility. The deployment will also add additional Unattended Ground Sensors.

- AJO-1 deployment: Will consist of the construction and placement of sensor and communication towers in the Ajo Station AOR. The deployment will also add additional Unattended Ground Sensors.

- Deployment of the Common Operating Picture into the TUSCON-1 and AJO-1 projects.

- Purchase and deployment of 1250 unattended ground sensors.

**Tactical Infrastructure**

Tactical infrastructure deployments along the Southwest Border have increased significantly during Fiscal Years 2007 and 2008.

- Over 70 miles of pedestrian fencing was deployed during Fiscal Year 2007.

- Over 55 miles of vehicle barriers were deployed during Fiscal Year 2007.

- End of Calendar Year 2008 goals include the deployment of approximately 185 miles of additional vehicle fencing and 225 miles of pedestrian fencing along the Southwest Border.

**Partnerships**

On the Southern border, CBP's Border Patrol partners with other DHS components, federal, state, and Tribal law enforcement agencies, and the Government of Mexico, to bring together resources and fused intelligence into a geographical area that has been heavily impacted by illicit smuggling activity. By partnering, DHS continues to have a significant positive effect combating the threat of domestic terrorism, illegal cross-border migration, and all related crime in the border environment.

- Operation Stonegarden
  - Operation Stonegarden is a DHS funded, Border Patrol led, operation designed to incorporate the services of State, Local, and Tribal (SLT) law enforcement agencies for the purpose of enhancing border security and preventing the entry of terrorists and terrorist weapons of mass effect while at the same time mitigating the conspicuous effects of human trafficking organizations.

- Operation Jump Start
  - On May 15, 2006, President Bush announced his plan to deploy up to 6,000 National Guard personnel for the first year along the United States border

8

with Mexico in support of CBP's comprehensive strategy for gaining control of our borders. The second year deployment is currently 3000 troops. The intent of the operation is to provide CBP's Border Patrol an immediate means to enhance border enforcement operations while Border Patrol increased its own internal enforcement resources through hiring additional Border Patrol agents, mission support personnel, and procuring and applying new technology and infrastructure. The result was Operation Jump Start, a sustained (2-year) DHS and Department of Defense (DOD) collaborative effort to increase border security while enhancing the Border Patrol's ability and capacity to achieve its mission.

- Border Enforcement and Security Teams
  - The Border Patrol is an active partner with Immigration and Customs Enforcement and other Federal, state, and local agencies in the BEST taskforces located throughout the southwestern border that were formed specifically to combat cross-border criminal activity and violence. Participation in the taskforces leverage Border Patrol knowledge of the border area with other agencies' investigative expertise.

- Border Security Operations Center (BSOC)
  - The BSOC is located in Austin, Texas. It acts as a fusion center for the State of Texas Department of Public Safety regarding border security issues. As a participating agency, the Border Patrol shares and maintains intelligence and coordinates operational planning with law enforcement agencies within the State of Texas. The BSOC identifies trends and patterns to establish multi agency enforcement methodologies aimed at disrupting alien smuggling organizations and drug trafficking organizations operating in the region.

- Border Violence Protocols (BVP)
  - BVP is a bi-national action plan to combat border violence and improve public safety and was signed by Secretary Michael Chertoff and Mexico's Secretary of the Interior, Carlos Maria Abascal Carranza. This action plan sets forth goals and objectives to ensure that the appropriate law enforcement agencies of the respective governments work together to provide an effective, comprehensive joint response to incidents of cross-border violence and crime.

- Operation Against Smugglers Initiative on Safety and Security (OASISS)
  - OASISS is a bilateral prosecutions program between the United States Government and the Government of Mexico. The program targets and prosecutes alien smugglers and human traffickers that smuggle aliens into the United States.

9

- Operation Streamline
  - Operation Streamline is a collaborative effort of multiple agencies (U.S. Attorney's Office, U.S. Marshal's Service, ICE) that utilizes criminal prosecution to deter illegal entries and gain, maintain and expand control of problematic areas.
  - The Chief Patrol Agent identifies and designates a 'zero tolerance zone' for all illegal entries and directs that all prosecutable aliens, regardless of nationality, apprehended within the geographic boundaries be processed for criminal prosecution and removal proceedings.

**Fraudulent Document Detection Updates**

CBP has implemented the following measures to enhance the CBP Officers ability to detect fraudulent documents. With the exception of the specialized equipment deployed in 2006 to the 11 Ports of Entry (POEs) (bullet 5 below), all other actions noted below were intended for CBP Officers at all POEs:

- 2004- Implemented mandatory 8 hours in fraudulent document detection for all CBP Officers.
- 2004- Distributed packets with sample training documents and Driver's License Identification Guides to all POEs.
- 2005- Printed and distributed the Pocket Guide Reference to Document Security Features and Printing Techniques.
- 2005-2006 - Inserted Fraudulent Document Training into all relevant cross training modules.
- 2006-Provided 11 POEs that have the highest rate of fraudulent document interceptions with advanced equipment to assist with the examination and detection of fraudulent documents.
  1. San Ysidro POE
  2. Calexico POE
  3. John F. Kennedy International Airport
  4. Newark International Airport
  5. Laredo POE
  6. El Paso POE
  7. Miami International Airport
  8. Los Angeles International Airport
  9. Dulles International Airport
  10. Nogales POE
  11. Atlanta International Airport
- 2006 - Inserted 12 hours of fraudulent document detection into the Advanced Admissibility Secondary Processing Training program.
- 2007 - Provided updated fraudulent document training modules to the CBP Academy for inclusion in their curriculum.
- 2007 - Provided Virtual Learning Center training on Machine Readable Visas
- 2007 - Implemented mandatory refresher fraudulent document training.

10

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

### Order by Mail or Phone

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

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

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

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

## Congressional Relations

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

## Public Affairs

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

PRINTED ON RECYCLED PAPER