United States Government Accountability Office

GAO

Report to Congressional Requesters

June 2010

BORDER SECURITY

Improvements in the Department of State's Development Process Could Increase the Security of Passport Cards and Border Crossing Cards

GAO-10-589

June 2010

BORDER SECURITY

Improvements in the Department of State's Development Process Could Increase the Security of Passport Cards and Border Crossing Cards

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-589, a report to congressional requesters

Why GAO Did This Study

In July 2008, the Department of State (State) began issuing passport cards as a lower-cost alternative to passports for U.S. citizens to meet Western Hemisphere Travel Initiative requirements. In October 2008, State began issuing the second generation border crossing card (BCC) based on the architecture of the passport card. GAO was asked to examine the effectiveness of the physical and electronic security features of the passport card and second generation BCC. This report addresses: (1) How effectively State's development process—including testing and evaluation—for the passport card and second generation BCC mitigates the risk of fraudulent use? (2) How are U.S. Customs and Border Protection (CBP) officers using the cards' security features to prevent fraudulent use at land ports of entry? To conduct this work, GAO evaluated the security features of passport cards and second generation BCCs against international standards and guidance and results from testing and evaluation and observed the inspection of these cards at five land ports of entry (POE).

What GAO Recommends

GAO recommends that State fully address any problems found during testing and evaluation, including documenting the reasons for not addressing any of them, and test and evaluate the security features on the cards as they will be issued. State agreed with the recommendations.

View GAO-10-589 or key components.
For more information, contact Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

State developed a passport card and second generation BCC that generally meet standards and guidance for international travel documents and include numerous, layered security features that, according to document security experts in the Department of Homeland Security, provide adequate security against fraudulent use. While following standards and guidance helps to ensure the security of these documents, State's development process could be improved. State addressed most problems identified during evaluation and testing; however, it did not address some of the resulting issues and recommendations or did not document its reasons for not doing so. In addition, State tested and evaluated the security of only prototypes of the passport card, which did not include key features such as the background artwork, personalization features, and other security features that were added or changed for the final passport card. Moreover, State did not test the security of the second generation BCC or the updated passport card expected to be issued in the second quarter of 2010. Fully testing the passport card and BCC and addressing identified problems would provide State a more complete understanding of the overall security and performance of its cards and a greater assurance that its cards are adequately secure.

CBP officers in primary inspection—the first and most critical opportunity to identify individuals seeking to enter the United States with fraudulent travel documents—use a variety of methods to identify fraudulent documents, but are unable to take full advantage of the security features in passport cards and BCCs because of time constraints, limited use of technology in primary inspection, and the lack of sample documents for training. While CBP has deployed technology tools for primary inspectors to use when inspecting passport cards and BCCs, it could still make better usage of fingerprint data to mitigate the risk of imposter fraud with BCCs, the most common type of fraud. In addition, although CBP provided training on security features of the passport card and second generation BCC to inspecting officers prior to their issuance, the conduct of training without sample passport cards or second generation BCCs at the Vermont POEs visited by GAO indicate that improvements are still needed. State and DHS need to fully implement GAO's prior recommendation to improve training on new documents prior to their issuance, including the provision of exemplars to be used during training to better familiarize officers with the look and feel of the actual documents.

Passport Card and Second Generation BCC

Passport Card

Second Generation BCC

Source: State Department.

Contents

Abbreviations

BCC	border crossing card
CBP	U.S. Customs and Border Protection
DHS	Department of Homeland Security
FDL	Forensic Document Laboratory
ICAO	International Civil Aviation Organization
ICE	U.S. Immigration and Customs Enforcement
ISO	International Organization for Standardization
L-1	L-1 Identity Solutions
NIST	National Institute of Standards and Technology
POE	port of entry
RFID	radio frequency identification
SPP	Security and Prosperity Partnership
US-VISIT	U.S. Visitor and Immigrant Status Indicator Technology
WHTI	Western Hemisphere Travel Initiative

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

June 1, 2010

The Honorable Howard L. Berman
Chairman
Committee on Foreign Affairs
House of Representatives

The Honorable Edolphus Towns
Chairman
Committee on Oversight and Government Reform
House of Representatives

The Honorable Brian P. Bilbray
The Honorable Christopher P. Carney
The Honorable Jane Harman
The Honorable Zoe Lofgren
House of Representatives

In response to section 7209 of the Intelligence Reform and Terrorism Prevention Act of 2004, the Department of Homeland Security (DHS) and the Department of State (State) implemented the Western Hemisphere Travel Initiative (WHTI). WHTI is an effort to require a passport or other document, or combination of documents, sufficient to denote identity and citizenship for all travel into the United States by U.S. citizens and by categories of individuals for whom documentation requirements had previously been waived. In July 2008, State began producing and issuing passport cards as a lower-cost alternative to passports for U.S. citizens to meet WHTI requirements at sea and land borders. The use of Border Crossing Cards (BCC)[1] by Mexican nationals to enter the United States at the land border from Mexico was unaffected by the implementation of WHTI.[2] In October 2008, State began producing and issuing a redesigned second generation BCC.

[1]BCCs are a form of nonimmigrant visa that allow approved Mexican nationals to enter the United States for business, pleasure, or medical treatment without additional documentation. Travel is limited to 25 miles from the U.S. border (75 miles if entering through certain ports of entry in Arizona) for fewer than 30 days.

[2]Regulations implementing WHTI require Mexican nationals to present a passport and visa when entering from Canada at the land border.

Considerable attention has been focused on the risks associated with the use of travel documents by noncitizens attempting to fraudulently enter the United States. Preventing, detecting, and responding to the fraudulent use of travel documents is essential to protecting U.S. citizens and interests at home and abroad. The integrity of legitimate travel documents is dependent upon the combination of well-designed security features and issuance and inspection processes that lead to detection of fraudulent attempts to obtain and use travel documents. In fiscal year 2009, more than 13,000 fraudulent border crossing cards and 4,500 fraudulent passports were intercepted by DHS's U.S. Customs and Border Protection (CBP) at all U.S. ports of entry (POE).[3] U.S. travel documents have been used fraudulently in connection with other crimes, including narcotics trafficking, alien smuggling, and even terrorism. State's Bureau of Consular Affairs issues passports and visas, including passport cards and BCCs, and CBP inspects these documents at ports of entry.

In response to your request, this report focuses on the effectiveness of the physical and electronic security features of the passport card and second generation BCC. Specifically, it examines the following two questions: (1) How effectively does State's development process—including procurement and testing and evaluation—for the passport card and second generation BCC mitigate the risk of fraudulent use? (2) How are CBP officers using the security features of passport cards and second generation BCCs to prevent fraudulent use at land POEs? To answer these questions, we evaluated the security features of passport cards and second generation BCCs and assessed the inspection of these cards at land POEs. We did not evaluate the issuance processes for these cards because they

[3]A port of entry is an officially designated location (airport, seaport, and land border locations) where CBP officers clear travelers for entry into the United States. There are 326 ports of entry.

follow the procedures for passport and visa issuance and we have completed recent work on these issuance processes.[4]

To determine how effectively State's development process for the passport card and second generation BCC mitigates the risk of fraudulent use, we interviewed officials from State's Bureau of Consular Affairs, CBP, and the Forensic Document Laboratory (FDL) in DHS's U.S. Immigration and Customs Enforcement (ICE). We interviewed State and DHS officials on the designs for the security features of the passport card and BCC and assessed them against applicable standards and guidelines. We also reviewed the results of testing and evaluation of the prototype passport cards conducted by the National Institute of Standards and Technology (NIST), FDL, CBP, the Bank of Denmark, and Sandia National Laboratory and reviewed how State and DHS used the results of the testing and evaluation activities. Finally, we interviewed officials at the Tucson Passport Center to understand and observe how second generation BCCs are personalized.

To determine how CBP officers use the security features of passport cards and second generation BCCs to prevent fraudulent use at land POEs, we interviewed officials from CBP and reviewed CBP policies, procedures, guidance, and training documents regarding the inspection of travelers presenting passport cards and second generation BCCs for the purpose of entry to the United States, including the use of the cards' physical security features and cardholder information retrieved from CBP border inspection systems. We conducted site visits to five land POEs in two port areas to interview CBP officials and observe the inspection process of travel documents to understand how CBP officers use the physical security features and DHS database information to verify the eligibility of a traveler presenting a passport card or BCC to enter the United States. See

[4]Recent GAO work on passport or visa issuance processes includes GAO, *Addressing Significant Vulnerabilities in the Department of State's Passport Issuance Process*, GAO-09-683R (Washington, D.C.: Apr. 13, 2009); *Department of State: Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process*, GAO-09-447 (Washington, D.C.: Mar. 13, 2009); *Border Security: State Department Is Taking Steps to Meet Projected Surge in Demand for Visas and Passports in Mexico*, GAO-08-1006 (Washington, D.C.: July 31, 2008); *Border Security: Security of New Passports and Visas Enhanced, but More Needs to Be Done to Prevent Their Fraudulent Use*, GAO-07-1006 (Washington, D.C.: July 31, 2007); and *State Department: Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts*, GAO-05-477 (Washington, D.C.: May 20, 2005).

appendix I for the POE selection methodology and further details on our scope and methodology.

We conducted this performance audit from January 2009 to June 2010, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

WHTI implements Section 7209 of the Intelligence Reform and Terrorism Prevention Act of 2004, as amended,[5] which requires DHS, in consultation with State, to develop and implement a plan to require U.S. citizens and other individuals for whom documentation had previously been waived to show a passport or other document, or combination of documents sufficient to denote identity and citizenship when entering the United States. DHS implemented WHTI documentation requirements at air ports of entry on January 23, 2007,[6] and at land and sea ports of entry on June 1, 2009.[7] The final land and sea rule provides that:

- U.S. citizens entering at sea or land POEs must present a valid U.S. passport, U.S. passport card, trusted traveler card, Merchant Mariner Document when traveling on official maritime business, or U.S. military ID when traveling on official orders;[8] and
- Mexican nationals applying for admission as a temporary visitor for business or pleasure may present a BCC in lieu of a passport to enter the United States when arriving from Mexico at land POEs or when arriving by pleasure vessel or ferry.

[5]Pub. L. No. 108-458, 118 Stat. 3638, 3823 (Dec. 17, 2004).

[6]*Documents Required for Travelers Departing From or Arriving in the United States at Air Ports-of-Entry From Within the Western Hemisphere; Final Rule*, 71 Fed. Reg. 68412 (Nov. 24, 2006).

[7]*Documents Required for Travelers Departing From or Arriving in the United States at Sea and Land Ports-of-Entry From Within the Western Hemisphere*, 73 Fed. Reg. 18384 (Apr. 3, 2008).

[8]Certain other documents may be presented by travelers on certain closed-loop cruises or by children under the age of 16.

State, in cooperation with DHS, is responsible for the development of passport cards and BCCs. The Bureau of Consular Affairs is responsible for the issuance of passport cards and BCCs, and CBP inspects the documents at ports of entry to the United States.

On December 31, 2007, State issued a final rule establishing the passport card as a lower-cost alternative to passport books —$45 for a passport card versus $100 for a passport book—for departure from and entry to the United States through land and sea ports of entry between the United States and Mexico, Canada, the Caribbean, and Bermuda.[9] The passport card cannot be used for international air travel. In February 2008, State began accepting applications for passport cards, and in March 2008, it awarded a contract to L-1 Identity Solutions (L-1) for passport card stock, personalization equipment, and related technical services. State began issuing the first generation passport card on July 14, 2008 and the updated second generation passport card in mid-April 2010. The passport card is valid for up to 10 years and only issued to U.S. nationals, using the same application form and evidence of citizenship or nationality as required for passport books.[10]

On October 1, 2008, State assumed responsibility for the production of BCCs, issuing a redesigned, second-generation BCC.[11] All first-generation BCCs will expire before October 2018. The design of the second generation BCC is based on the construction and security features of the passport card. State uses the same contract to procure BCC cardstock and the personalization equipment can be used to personalize both types of cards. The BCC is valid for up to 10 years and is only issued to Mexican citizens.[12]

[9]*Card Format Passport; Changes to Passport Fee Schedule; Final Rule*, 72 Fed. Reg. 74169 (Dec. 31, 2007).

[10]A passport card, for individuals 16 years or older, is valid for 10 years from the date of issuance; it is valid for 5 years for younger travelers.

[11]From April 1998 until DHS assumed responsibility for its functions in March 2003, the Immigration and Naturalization Service produced the first generation border crossing card, also known as a laser visa, and DHS's U.S. Citizenship and Immigration Services produced the laser visa from March 2003 until October 2008.

[12]A border crossing card, for individuals 15 years or older, is valid for 10 years from the date of issuance; as of June 4, 2010, for younger travelers, it is valid up to the 15th birthday or 10 years, whichever comes first.

The passport card and second generation BCC use vicinity radio frequency (RF) technology to store and transmit a unique number that can be used by CBP to retrieve information about the cardholder.

As amended, the Intelligence Reform and Terrorism Prevention Act of 2004 required DHS and State to certify that they have met certain criteria prior to implementing WHTI documentation requirements at sea and land borders, including:

- NIST certification that the passport card architecture meets or exceeds International Organization for Standardization (ISO) security standards and best practices for protection of personal information;
- making the passport card available to U.S. citizens; and
- installing the infrastructure to process the passport cards and training employees to use the new technology at ports of entry.

State and DHS certified that they met these conditions on February 24, 2009.

The security of passport cards and BCCs and the ability to prevent and detect their fraudulent use are dependent upon a combination of well-designed security features and inspection procedures that utilize the available security features of the document. A well-designed document has limited utility if inspectors do not inspect the security features to verify the authenticity of the document. In 2007, we reported on the security of passports and visas, including first generation BCCs. In our report, we made several recommendations to State and DHS regarding the planning and design process for its travel documents, ensuring that needed technology is available at ports of entry, and better training for CBP officers at the ports of entry.[13]

Passport Card and Border Crossing Card Fraud

Threats to the security of travel documents include counterfeiting of a complete travel document, construction of a fraudulent document, photo substitution, deletion or alteration of text, removal and substitution of pages, theft of genuine blank documents, and assumed identity by

[13]GAO, *Border Security: Security of New Passports and Visas Enhanced, but More Needs to Be Done to Prevent Their Fraudulent Use*, GAO-07-1006 (Washington, D.C.: July 31, 2007).

imposters. Features of travel documents are assessed by their capacity to secure a travel document against the following:

- Counterfeiting—unauthorized construction or reproduction of a travel document.
- Forgery—fraudulent alteration of a travel document, including attacks such as photo substitution, and deletion or alteration of text.
- Imposters—use of a legitimate travel document by people falsely representing themselves as legitimate document holders.

Most reported passport card and BCC fraud is imposter fraud. In fiscal year 2009, CBP detected 13,530 passport cards and BCCs presented by travelers attempting to enter the United States through all U.S. POEs that were either fraudulent or were valid documents used by imposters (see table 1). Over 90 percent of these documents were genuine documents presented by imposters. The most frequent fraudulent attempts were by imposters attempting to use a legitimate BCC. Fraudulent use of passport cards and second generation BCCs is much lower than that of first generation BCCs mainly because there are many fewer issued, with over 8 million valid first generation BCCs in circulation but only about 2.3 million passport cards and 435,000 second generation BCCs issued by the end of November 2009.

Table 1: Number of Fraudulent U.S. Passport Cards and BCCs Detected at U.S. Ports of Entry, Fiscal Year 2009

Travel document	Imposter	Counterfeit/altered	Total
Passport card	43	0	**43**
First generation BCC	12,318	987	**13,305**
Second generation BCC	170	12	**182**
Total	**12,531**	**999**	**13,530**

Source: GAO analysis of DHS and State data.

Document Security Features

To combat document fraud, security features are used in a wide variety of documents, including currency, identification documents, and bank checks. Security features are used to prevent or deter fraudulent alteration or counterfeiting of such documents. In some cases, an altered or counterfeit document can be detected because it does not have the look and feel of a genuine document. For instance, in U.S. passport cards and second generation BCCs, detailed designs and figures with specific fonts

and colors can often be used by inspectors to identify nongenuine documents.

While security features can be assessed by their individual ability to help prevent the fraudulent use of the document, it is more useful to consider the entire document design and how all of the security features combine to help secure the document. Layered security features tend to provide better security by minimizing the risk that the compromise of any individual feature of the document will allow for unfettered fraudulent use of the document. An individual security feature may provide protection against more than one type of threat, but no feature can protect against them all and no single feature is 100 percent effective at eliminating a type of threat. Designing secure documents requires the use of a range of security features combined in an appropriate way within the document. The best protection is obtained from a balanced set of features and techniques providing multiple layers of security in the document that combine to deter or defeat fraudulent attack.

Card Application and Issuance Processes

The application and issuance process for the passport card is the same as for passports, using the same application form. After an application is successfully adjudicated by passport examiners at State Department passport agencies, the passport card will be produced. State personalizes each passport card by printing the photo, biographical data, and other needed information on the card. The card is then mailed to the traveler. In general, passport cards are personalized at State's Arkansas Passport Center, but the Tucson Passport Center also has the capacity for high volume personalization of the cards and most passport agencies have the capability of personalizing limited volumes of cards.

The application and issuance process for the BCC is unchanged for the second generation BCC and is managed through the U.S. consulates in Mexico. After visa officers in Mexico approve an application for a BCC, the BCCs will typically be produced at the Tucson Passport Center. Using blank BCC cardstock, State personalizes each BCC by printing the photo, biographical data, and other needed information on the card. The card is then delivered to the appropriate consulate in Mexico for issuance to the traveler.

In each case, the cardstock is produced by one of L-1's subcontractors and it incorporates the background art and some of the security features already incorporated. As will be explained later in this report, some security features are added to the card during the personalization process.

Inspection of Travel Documents to Enter the United States

In general, travelers seeking admission to the United States must present themselves and a valid travel document for inspection to a CBP officer. The inspection process requires officers to determine the admissibility of the traveler by questioning the individual and inspecting the presented travel documents. In the first part of the inspection process—primary inspection—CBP officers inspect travelers and their travel documents. The officer can then compare the information on the travel documents with information retrieved from CBP border inspection systems to determine if they may be admitted or should be referred to secondary inspection for further questioning and document examination. If additional review is necessary, the traveler is referred to secondary inspection—an area away from the primary inspection area—where another officer makes a final determination to admit the traveler or deny admission for reasons such as the presentation of a fraudulent or counterfeit travel document.

State's Development Process Resulted in Cards That Generally Meet Standards and Guidance for International Travel Documents, but Improvements Could Be Made

State's designs for the first and second generation passport card and the second generation BCC generally meet standards and guidance for international travel documents and DHS policies for travel credentials and, in general, the recommended security features that are not included are compensated for by other security features or would not greatly increase the security of the cards.[14] However, while including all security features recommended by guidance and standards for international travel cards can help ensure the security of passport cards and BCCs, security assessments and testing of the cards are necessary to identify any vulnerabilities and to modify the security features to address these vulnerabilities. During its development process, State addressed most of the issues raised and recommendations made during evaluation and testing of the prototype passport card, but it either did not address some of the issues and recommendations, or it did not fully document its decisions for not doing so. Moreover, State tested and evaluated the security and durability of only prototypes of the passport card, which did not include the personalization printing or background artwork. Without fully evaluating the impact of the issues and recommendations on the security and performance of the cards and testing and evaluating the final designs for the first and second generation passport card and second

[14]For the purpose of this report, the designs of the passport card and second generation BCC encompass the physical construction of the cards, as well as other features added by the manufacturer and State.

generation BCC, State does not have a complete understanding of the cards' overall security and performance.

Passport Cards and Second Generation BCCs Generally Meet International Travel Documents Standards and Guidance

The passport card and second generation BCC generally meet International Civil Aviation Organization and Security and Prosperity Partnership standards, as well as the DHS Policy for Physical Security Features, for international travel documents. These documents provide guidance on security features and data elements to include on travel documents to prevent fraudulent use.

Card Designs Generally Meet International Civil Aviation Organization Security Standards for Machine Readable Travel Documents

The International Civil Aviation Organization (ICAO)—the United Nations specialized agency for civil aviation—document 9303 on machine-readable travel documents provides standards for passports and other travel documents that can be used for international travel, including recommended security standards and data elements for travel documents.[15] The recommended security features are divided into two categories, basic security features that are considered essential and additional features recommended for enhanced security. The passport card includes 8 of approximately 11 ICAO recommended basic security features and the BCC includes 7 of the 11 basic security features. However, the security that would be offered by the missing features is either provided by other security features or would not significantly improve the security of the cards. Both cards contain many of the recommended additional features. Table 2 provides further details about the missing ICAO basic security features and the factors on the cards that mitigate their omission. The ICAO standards also provide data element requirements for the personalization of travel documents. The passport card contains 10 of the 11 required data elements and second generation BCC contain 9 of the 11 required data elements. Neither card contains the signature of the cardholder, which does not significantly impact the security of the cards because signatures are easy to forge and thus provide little protection against document fraud. In addition, the second generation BCC lacks a document number on its biographical face, which is both a security feature and data element. There is, however, a unique inventory control stock number on the back of the card. While the

[15]ICAO, *Machine Readable Travel Documents*, *Part 3 Machine Readable Official Travel Documents*, *Volume 1*, *MRTDs with Machine Readable Data Stored in Optical Character Recognition Format*, ICAO 9303 Part 3, Third Edition (2008).

presence of a unique identifier is important, the location does not play a major role in the overall card security.

Table 2: Missing ICAO-recommended Basic Features and Mitigating Factors

ICAO-recommended basic security feature	Reasons why the missing feature does not significantly impact the security of the documents
Two-color guilloche pattern to protect against copying[a]	A guilloche pattern is incorporated in the optically variable device (OVD), which displays kinematic and rainbow effects as the angle of viewing is changed.[b] This provides a higher level of counterfeit resistance than the traditional two-color guilloche pattern
Anti-scan pattern to protect against copying	Features such as the OVD and optically variable logo provide similar protection.
Ultraviolet fluorescent ink on both sides	An ultraviolet image is printed on the front of the cards but not on the back. The overall security of the cards is not negatively affected because the primary threat is the alteration of biographical data on the front of the cards.
Unique document number on second generation BCC	There is a unique inventory control stock number on the back of the card. While the presence of a unique identifier is important, the location does not play a major role in the overall card security.

Source: GAO analysis of ICAO standards and State's designs for the passport card and second generation BCC.

[a]A guilloche pattern consists of continuous fine lines that form a unique image that is difficult to copy or recreate without access to the originating equipment, software, and parameters used to create the original design.

[b]OVDs significantly change appearance depending on the angle of illumination and observation and are designed to prevent copying by photomechanical means.

Card Designs Generally Meet Security and Prosperity Partnership Recommended Standards for Secure Proof of Status and Nationality Documents to Facilitate Cross-Border Travel

The Security and Prosperity Partnership (SPP)—an effort among the United States, Canada, and Mexico to develop a common security strategy—developed *Recommended Standards for Secure Proof of Status and Nationality Documents to Facilitate Cross-Border Travel* to align with ICAO document 9303, which provide recommended nonbinding minimum standards and, for additional measures of security, best practices for documents used for travel between the United States and Canada.[16] Both the passport card and BCC generally meet SPP recommended standards. Both cards include all 6 of the security features required to meet the minimum standard. The passport card contains all 9 of the data elements required to meet the minimum standard and the

[16]Security and Prosperity Partnership Traveler Screening Systems Working Group, *Recommended Standards for Secure Proof of Status and Nationality Documents to Facilitate Cross-Border Travel* (February 2007).

second generation BCC contains 8 of the 9 data elements required to meet the minimum standard. In addition, the cards include many security features recommended as a best practice. The second generation BCC does not have the document version data element, which indicates to inspectors the version of the document they are inspecting so that they know what the card should look like and what security features it should have. However, this is not a concern because the second generation BCC looks completely different from the first generation BCC.

Card Designs Generally Meet DHS's Policy for Physical Security Features

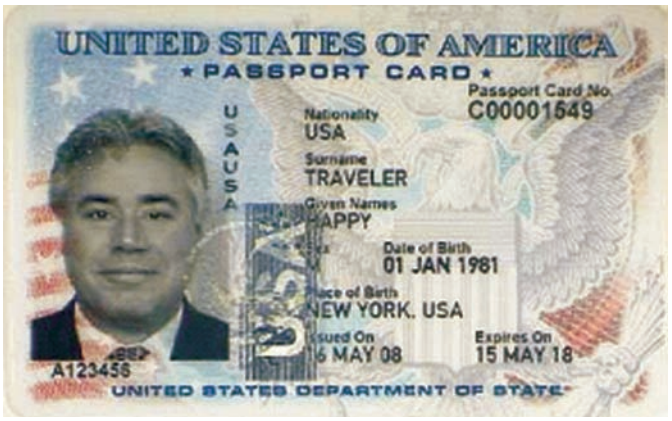
The DHS Screening Coordination Office created the DHS Policy for Physical Security Features as a result of its efforts to identify how DHS can improve its credentialing programs. The policy addresses physical security features that prevent counterfeiting, alteration, and fraud of credentials and provides a minimum standard for physical security features for DHS credentialing programs, including requiring a minimum of two security features. The policy also includes requirements for data elements for travel documents to enable border officers to assess the identity and admissibility of travelers. The passport card and BCC contain all required security features, the passport card contains 10 of the 11 required data elements, and the BCC contains 9 of the 11 required data elements for the travel environment specified in the policy. Neither card contains height information and the second generation BCC does not include the cardholder's place of birth. Not including these data elements does not significantly affect the security of the cards because the cards contain layers of security to protect against fraudulent use. DHS plans to remove both height and place of birth as a minimum requirement in the next version of its policy.

Layered Features Contribute to Overall Security of Passport Cards and Second Generation BCCs

The designs of the passport card and BCC contain numerous, layered features that provide protection against fraudulent use (see figs. 1 and 2). For example, the OVD can help protect against counterfeiting because it is difficult to copy and recreate and it helps protect against forgery because it overlaps the photograph and biographical data, making it difficult to alter them without causing visible damage to the OVD. In addition, the complex symbolic codes and pseudocodes provide protection against counterfeiting and forgery because they are based on cardholder characteristics and cannot be accurately created for counterfeit cards or altered for forged cards unless the counterfeiter has broken the codes. Laser engraving is used to print the cardholder's image as well as the personalization information, combining flat and tactile printing. Laser engraving permanently blackens the plastic below the surface of the card

to protect against counterfeiting and forgery by making it difficult to alter without causing damage.

Figure 1: Front and Back of Passport Card



Front of U.S. sample passport card

Back of U.S. sample passport card

Source: State Department.

Figure 2: Front and Back of Second Generation BCC

Front of second generation BCC

Back of second generation BCC

Source: State Department.

In meetings between GAO and FDL on the security of the final passport card and second generation BCC designs after State had begun issuing the cards, FDL officials indicated that they believed that the security of the final cards against fraud is adequate. However, they continue to recommend that State use a solid polycarbonate body with laser engraving at or below the layer of background artwork to provide stronger protection against layer separation, photo substitution, and data alteration, as they had recommended when they performed the counterfeit deterrence study on the prototype passport cards during procurement.[17]

FDL also recommended to State, based on reviewing an intermediate printing of the passport card, that it add rainbow printing on the front of the card, which would make the card more difficult to copy and counterfeit.[18] Regarding the second generation BCC, which they had not formally assessed, FDL officials suggested using a more easily recognizable, finite design for the background of the BCC, like the eagle on the passport card. It

[17]Counterfeit deterrence studies involve reviewing prototype security documents using scientific instrumentation for their adherence to recognized security printing standards, technologies, and methods. Conclusions are based on real world experience with compromised documents.

[18]Rainbow printing produces artwork with a gradual color change across the card surface.

is easier to see a poor reproduction of a well-known, finite design than an abstract one, like the butte on the BCC.

State officials said that they respond to recommendations based on whether the cost justifies the security benefit gained as well as potential program delays that may result from implementation. They indicated that they did not change to a solid polycarbonate body because there are problems using polycarbonate in the radio frequency identification (RFID) chip layer and it would increase the cost of the cards.[19] In addition, at the time, the card manufacturer thought that the technology for security printing on polycarbonate was too new and State didn't believe that using layers of polycarbonate over layers of polyvinyl chloride posed any significant problems. Since procurement, the technology for laser engraving and printing the background artwork on polycarbonate has improved, but there continue to be technical issues that impact the feasibility of its use. State also does not believe that laser engraving below the layer of the background artwork significantly improves the security of the cards because any attempt to alter the data or photo would visibly damage the card. In addition, State officials believe the recommendation to add rainbow printing on the front of the cards is more a preference than a requirement and is satisfied with having it just on the back of the cards. State officials have indicated that they will consider FDL's suggestion for a finite design for the background of the BCC when they design new documents or redesign the existing ones.

State's Development Process for Passport Cards and Second Generation BCCs Could be Improved

At the beginning of the development process for the passport card, State investigated available security technologies and worked with DHS, including CBP and FDL, to determine which physical security technologies and features to require for passport cards. These included laser engraving printers for personalization, tactile element(s) over the photo area, a logo with color shifting ink, and an optically variable device either provided by State or proposed by vendor. In addition, State, based on input from DHS, included a vicinity read RFID chip to facilitate faster processing at ports of entry. The RFID chip stores a unique number that references cardholder information in State's issuance databases. State also determined that the cards must comply with ICAO recommendations for card format official

[19]An RFID chip contains a unique number that can be read remotely. For passport cards and second generation BCCs, this unique number references cardholder information in State and DHS databases.

travel documents.[20] These requirements were incorporated into the procurement solicitation issued in May 2007.

The source selection and procurement process began when State developed the request for proposal (RFP), which was released in May 2007. The contract was awarded to L-1 in March 2008 for passport cards.[21] During the source selection and procurement process for passport cards, prototype passport cards from prospective contractors underwent evaluation and testing related to durability, RFID performance, and security requirements. Sandia National Laboratory (Sandia) evaluated the durability and radio frequency (RF) effectiveness against national and international standards; CBP tested the RFID performance in mock CBP vehicle lanes; and FDL performed counterfeit deterrence studies. State implemented most of the recommendations made and addressed most of the issues raised during evaluation and testing. For example, in response to FDL recommendations, State embedded the OVD below the surface of the card and included microline printing in the background artwork. In addition, State either amended the RFP based on NIST's recommendations or provided a written reason why a recommended change was not made.

While State addressed most of the issues raised and recommendations made during evaluation and testing of the prototype passport card, it either did not address some of the issues and recommendations or did not document its reasons for not doing so. For example, State did not assess the risk of not following FDL's recommendation that State submit the final passport card for analysis of the security features, which State did not do because it was in the final stages of procurement when the design was finalized and it wanted to meet schedule, or FDL's recommendation that it add rainbow printing to the front of the card. State also did not assess the potential risk posed by the card's failure to meet peel strength and ultraviolet light exposure test requirements that were found during Sandia's tests prior to the issuance of the cards. While State officials do not believe that the problems identified by the failed tests will affect the operational use of the cards, they were not able to explain why these failures were not assessed prior to decisions to proceed with card production. Moreover, State assessed, but did not document its reasons for not addressing FDL's concern that the shallow depth of the laser

[20]ICAO 9303, Part 3, Volume 1.

[21]The contract was initially awarded to General Dynamics Information Technology in January 2008. By mutual agreement, this contract was terminated.

engraving left the cards susceptible to alteration and recommendation to use a solid polycarbonate body to mitigate this. State officials decided not to follow the recommendation to use a solid polycarbonate body based on the costs and benefits of implementing it; they believe that the depth of the laser engraving was sufficient and decided against using a solid polycarbonate body due to cost and technical issues. Without performing and documenting a full assessment of recommendations made and problems found during testing and evaluation, including the potential effect not addressing them could have on the performance of the card, State does not fully understand the security and durability of the card.

After awarding the contract for passport cards, the contractor manufactured cards according to State's final design, which were made into exemplars—genuine documents used for training purposes. These cards were inspected for problems with the security features and printing and any problems were recorded. Some of the cards were also sent to CBP to test the RFID performance. State indicated that it encountered a small percentage of manufacturing problems and the cards met CBP RFID performance requirements. The second generation BCC underwent similar inspection of the security features and printing after it was added to the passport card contract and manufacturing began.

State designed the background artwork as well as codes that are embedded into both the passport card and BCC during personalization. These codes vary between the passport card and BCC, with the BCC containing more codes with greater depth and complexity because it was produced later, providing State with more time to develop them. The codes are based on the holder's personal information. The simplest codes can be used for document authentication by primary inspectors and the most complex codes can be used for forensic analysis.

While testing and evaluation was performed on prototype passport cards during the source selection process, these activities did not assess security features designed by State, including the background artwork or embedded personalization codes. The focus of the test and evaluation activities was to evaluate offerings from prospective contractors. Security features that were added or changed from the prototype passport cards and incorporated into the final passport card were also not evaluated and durability testing was not performed on the final design, despite failures encountered during testing. Further, because the second generation BCC was added to the passport card contract, it did not undergo any formal security testing and evaluation activities and no security or durability testing was done on the second-generation passport card, which includes

changes to the card construction due to the inclusion of a different RFID chip. The background artwork and the security features added during the personalization process are key components of the layered security of the passport card and second generation BCC. However, without tests or evaluations that demonstrate the ability of these features to effectively contribute to the security of the cards, State does not have the needed assurance that its cards have been designed with adequate security.

State has completed a redesign of the passport card with the primary purpose of incorporating a new RFID chip that has a unique tag identifier.[22] The use of the unique tag identifier is intended to prevent cloning of the RFID chip. State took the opportunity to incorporate changes to improve the physical security features of the card, including using more robust layers of pseudocodes that bring them to the depth and complexity of those used on the BCC and a more complex OVD. The updated card also contains additional physical security features, including a secondary image of the cardholder and steganography in the primary image and microprinting in the secondary image of the cardholder.[23] State began issuing the second generation passport card in mid-April 2010.

The redesigned card has not undergone formal security or durability testing and evaluation. State officials believe that evaluation activities were not necessary because the appearance of the card is so similar to the one currently issued, the changes improved the security of the card, and it did not consider the durability failures encountered during prototype passport card testing to be significant. In 2007, we recommended that State periodically reassess the security features when planning the redesign of its travel documents.[24] State agreed with the recommendation and has taken steps to address it. However, there was no assessment of the final passport card or second generation BCC prior to issuance and there is no plan to formally assess the second generation passport card prior to issuance. Such an assessment could identify potential vulnerabilities in the security of these

[22]A unique tag identifier is a universally unique number assigned by a registration authority to the chip manufacturer plus a unique serial number issued by the manufacturer. It is written permanently at the time the chip is manufactured and cannot be changed or cloned.

[23]Steganography is a technique of concealing data into a document, usually in the cardholder's portrait or background security printing that can only be seen when viewed with a special lens or detected by specialized software. In the second generation passport card, codes are embedded in the primary image of the holder and are only visible using a viewing device.

[24]GAO-07-1006.

cards before they could be exploited. There have been no reports of successful fraudulent use of the cards and the addition of more security features to the passport card was not in response to any threats or vulnerabilities and should further strengthen the card against fraud. State and FDL inspected counterfeit second generation BCCs that were intercepted and found that none of the security features or personalization codes had been compromised. However, by not following a structured process for assessing the security features of the passport card prior to issuing the second generation passport card, State missed an opportunity to identify and address any potential vulnerabilities of the passport card's design to resist fraudulent use.

In response to our 2007 recommendation, State created a new position in the Bureau of Consular Affairs responsible for the coordination of the efforts of various State organizations involved in designing and ensuring the security of documents issued by Consular Affairs—the Forensic Document Design and Integrity Coordinator. Because this position was created in September 2009, the coordinator was not involved in the development process of the first-generation passport card or the second generation BCC card and was only minimally involved in the development process of the second-generation passport card—only providing input to the post-production processes.

CBP Officers Use a Variety of Methods to Detect Travel Document Fraud, but Limitations in the Use of Technology and Training Affect Their Ability to Fully Utilize the Document Security Features

The inspection of passport cards and BCCs at POEs is a key element in preventing the fraudulent use of these documents. Inspection officers rely on interviews and observations of travelers and the examination and verification of documents using CBP border inspection systems to detect fraud. To aid in the inspection of passport cards and second generation BCCs, CBP deployed RFID readers and new software in vehicle lanes at land ports of entry. However, the limited amount of time officers have to conduct inspections restricts the use of security features on passport cards and BCCs to just a few visual and tactile features. Greater use of biometrics of travelers presenting BCCs could provide additional verification that the BCCs are valid and belong to the travelers presenting the documents, helping to address imposter fraud. Further, while CBP officer training on the passport card and BCC was timely, the provision of exemplars to the ports of entry for training purposes is still lacking. The CBP port director—responsible for supervising and directing all work activities at POEs—of the POEs we visited along the Northern border indicated that the POEs there did not have exemplars of either card. Without exemplars available during training, these officers were unable to

fully familiarize themselves with the look and feel of the security features in these documents before inspecting them.

Inspection Officers Rely on Interviews and Observations of Travelers, Examination of Documents, and Traveler Information Stored in CBP Border Inspection Systems to Detect Fraud

CBP officers in primary inspection rely on interviewing and observing travelers, visually and manually examining documents, and accessing cardholder information, such as the traveler's name and photo, in CBP border inspection systems to detect fraudulent passport cards and BCCs. CBP officers observe travelers' demeanor, question them about their travel, and compare travelers with biographic data and photos on travel documents and in CBP inspection systems to help them detect fraud. Officers inspect only a limited number of security features on travel documents due to time constraints, particularly along the southern land border where there is high traveler volume through many land border POEs. When inspecting documents, they look for signs of alteration, compare the photo and traveler, examine the biographic page and examine the look and feel of the document to determine whether it is valid. If the officer suspects fraud, they can send travelers to secondary inspection for further screening and, in the case of BCC holders, a comparison of traveler fingerprints with those stored in the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT), one of the CBP border inspection systems, to verify their identity.

DHS Deployed New Technology Systems at Ports of Entry to Aid in the Inspection of Passport Cards and Second Generation BCCs

To aid in the inspection of passport cards, second generation BCCs, and other travel documents with vicinity RFID chips, CBP made two related technology deployments to its ports of entry. First, it upgraded the client software to its border inspection systems at vehicle and pedestrian lanes at land border ports of entry. The vehicle primary client software provides a graphical user interface for CBP officers to access U.S. visa and passport information, including the traveler's photograph. State provides the information to CBP border inspection systems from its issuance databases: the Consular Consolidated Database for visas, including BCCs, and the Passport Information Electronic Retrieval System for passports and passport cards. Access to this information allows for better identification of fraudulent photos, biographical data alteration, or counterfeit cards. The vehicle primary client software is operational in most vehicle lanes at all but two land border ports of entry. CBP upgraded the pedestrian client software, which already provided access to visa information, to display passport information.

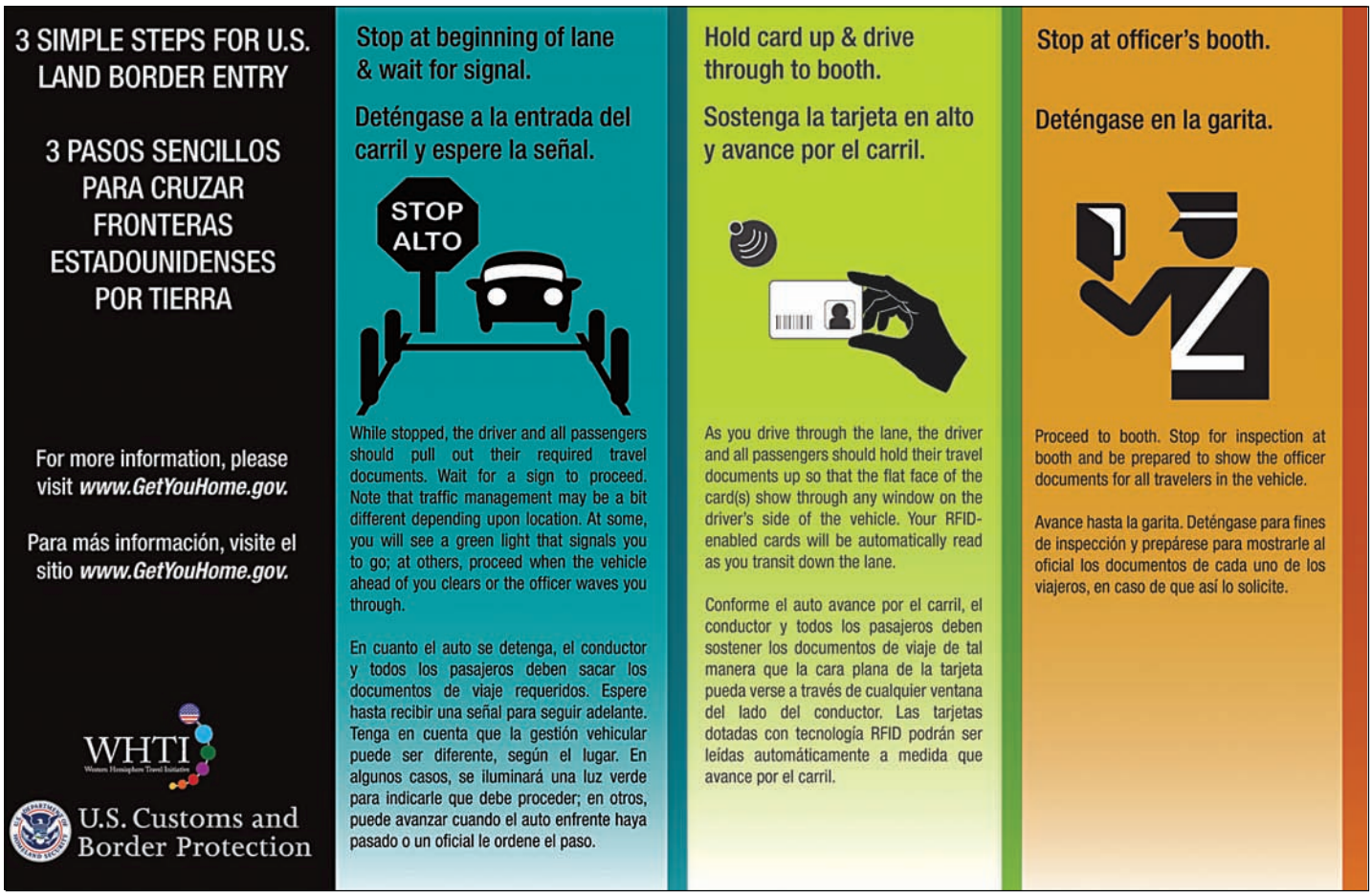
Second, CBP deployed RFID readers in vehicle lanes at land border ports of entry that can read the RFID chips in the passport card, second generation BCC, and other WHTI-approved documents. WHTI has

deployed RFID to 420 lanes at the top 46 land border POEs, which handle more than 95 percent of land border traffic. Travelers can hold up their passport card or second generation BCC when entering vehicle lanes at these POEs to allow RFID readers to read the RFID tag in the cards.[25] The RFID system then automatically looks up traveler's information from CBP border inspection systems and presents it to inspecting officers on the Vehicle Primary Client.

CBP has installed signage in RFID reader-equipped vehicle lanes and provides WHTI tear-sheets that are available in English, Spanish, and French that instruct cardholders on how to use RFID-enabled documents, which includes passport cards and BCCs (see fig. 3). In addition, State includes a letter in Spanish with BCCs containing instructions on how to use the cards at POEs.

[25]The RFID readers can also be used to read the RFID tag on CBP's trusted traveler cards, including NEXUS, Secure Electronic Network for Travelers Rapid Inspection (SENTRI), and Fast and Secure Trade (FAST).

Figure 3: WHTI Tear Sheet with Instructions on the Use of RFID-enabled Cards in English and Spanish



Source: Department of Homeland Security.

When a vehicle enters a vehicle lane at a port of entry, the occupants can see signs instructing them on how to hold RFID-enabled documents to allow them to be read (see fig. 4). The RFID reader attempts to read any RFID-enabled documents in the vehicle. The vehicle then approaches the booth where the CBP officer inspects the occupants' travel documents. If one or more of the documents was not read, whether because there was a read failure or one or more of the documents are not RFID-enabled, the CBP officer can read the RFID tags of any RFID-enabled document with an RFID reader at the booth, read the machine readable zone of any valid travel document with a document reader in the booth, or manually look up travelers' information using the data printed on the documents.

Figure 4: Signage for Use of RFID-enabled Cards at Vehicle POE

Sign in French

Sign in Spanish

Source: GAO.

In pedestrian lanes, a traveler presents his or her travel document to the CBP officer who can inspect it and look up the traveler's information by either electronically reading the machine readable zone of the travel document with a document reader or manually looking up the travelers' information.[26] The officer can then compare the information on the travel documents with information retrieved from CBP border inspection systems and with the traveler being inspected to determine if they may be admitted or should be referred to secondary inspection for further questioning and document examination.

[26]Machine readable zone document readers are operational in vehicle and pedestrian lanes at all land border ports of entry.

Limitations in the Use of Technology and Inspection Time Restrict the Use of Security Features in the Inspection of Passport Cards and BCCs

Officers in primary inspection—the first and most critical opportunity at U.S. ports of entry to identify individuals seeking to enter the United States with fraudulent travel documents—are unable to take full advantage of the security features in passport cards and BCCs due to the limited use of technology in primary inspection.

In our prior work examining the inspection of travel documents at POEs, we found that, due to time constraints and the large volume of travelers, primary officers inspect only a limited number of security features on travel documents and only electronically read travel documents to query records in CBP border inspection systems when deemed appropriate for the inspection situation, given the local traffic flow and traveler wait times.[27] CBP officers often rely on a few visual and tactile security features of the passport cards and BCCs—such as raised printing and the embossed seal—in addition to their interviews to identify fraudulent use of the documents. When visiting POEs along the Northern and Southern borders, CBP port directors told us that they are able to authorize less than 100 percent handling of travel documents and the port director of the POEs we visited on the Southern border told us he can authorize less than 100 percent electronic reading or manual lookup of travel documents during times of heavy traffic to mitigate long waits, although this happens only rarely in the POEs we visited on the Northern border. During our visits to POEs on the Northern and Southern borders, we observed 100 percent handling and electronic reading of travel documents. However, in 2008, only about 49 percent of travel documents were machine read in vehicle primary inspections, while in 2009 about 63 percent were read. Part of this increase may be attributed to the decrease in vehicle traffic during that period. According to CBP crossing estimates for vehicle lanes indicate, there was about a 10 percent decrease in vehicle traffic across the border between 2008 and 2009.

In our prior work examining the security of BCCs, we found that DHS was not fully utilizing the biometric features of the BCCs—that is fingerprint data—and recommended that DHS develop a strategy for better utilizing these features.[28] At the time, we found that only a small percentage of travelers with BCCs are referred to secondary inspection where their

[27] GAO-07-1006 and *Document Security: Additional Actions Needed to Assess Risk and Enhance Security of DHS Travel and Immigration-Related Documents*, GAO-08-505SU (Washington, D.C.: May 15, 2008).

[28] GAO-07-1006.

fingerprints can be compared to those in US-VISIT. These checks are usually performed only if a primary officer determines travelers are traveling beyond the geographic limits or exceeding the number of travel days allowed for use of the BCC, or if there are concerns about the traveler. The use of biometric checks of travelers presenting BCCs provides additional verification that the travel documents are valid and belong to the travelers presenting the documents, helping to address imposter fraud—the most significant type of fraud associated with BCCs. In fiscal year 2009, CBP officers intercepted over 12,000 BCCs used by imposters. Even with the second generation BCC, imposter fraud is much more common than fraud cases where the card has been counterfeited or altered. In fiscal year 2009, 170 cases of imposter fraud were detected with the second generation BCC while only 12 cases of altered or counterfeit second generation BCCs were detected. While the deployment of the Vehicle Primary Client to CBP land POEs provides officers more information on BCC holders, imposter fraud remains a significant risk.

In 2008, CBP developed a Mission Need Statement for U.S. Pedestrian Biometric Deployment to provide an additional security check at land border POEs, whereby existing single-print readers, which scan 1 fingerprint for comparison with the cardholders fingerprint information stored in the CBP border inspection systems, currently being replaced with 10-print readers, which scan all 10 fingerprints for comparison, in secondary inspection would be reallocated to pedestrian primary lanes to enable inspecting officers with suspicions of a BCC holder's identity to verify the individual against fingerprint records. As of March 2010, these systems have been deployed to all 136 pedestrian lanes at POEs across the southwest border. However, CBP only has only plans to install them at select vehicle lanes at remote POEs that have both vehicle and pedestrian lanes. CBP indicated that there are operational challenges to implementing biometric verification at busy POEs, which make secondary inspection the most efficient place to perform biometric verification.

CBP Officer Training on New Travel Cards Was Timely, but Exemplars Were Not Available at All Ports of Entry

Previously, we recommended that State and DHS collaborate to provide CBP inspection officers with better training for the inspection of documents issued by State, including training materials that reflect changes to State-issued travel documents and the provision of exemplars prior to issuance. State and DHS agreed with the recommendation and have taken steps to address it. For example, CBP provided training to

inspection officers on the passport card and second generation BCC prior to their issuance and provides continuing information to officers on document fraud. This training is done during musters[29] that include materials such as Fraudulent Document Analysis Unit[30] bulletins on document security features and counterfeit documents and exemplars of the documents; as part of other training done by CBP for inspecting officers; through conferences; and through access to online information on the documents. CBP officials also indicated that they provided exemplars of the passport card and second generation BCC to all POEs to train CBP officers prior to the cards' appearance at the POEs. However, while CBP officials at POEs we visited along the Northern and Southern borders indicated they had received training on the passport card and second generation BCC, officials at POEs along the Northern border indicated that they did not receive exemplars of either card and hence were unable to include them in their training of their officers. In our prior work, we found that the use of alerts and bulletins alone do not provide officers with an understanding of the look and feel of the actual documents. While State and DHS have taken positive steps in response to our recommendation to improve its training of officers on travel documents, the lack of exemplars at the POEs along the Northern border indicates that improvements are still needed. As State continues to update its travel documents, we continue to believe that State and DHS need to fully implement our prior recommendation to improve training of its officers on new documents prior to their issuance, which includes the provision of exemplars so that they can be used during training to better familiarize officers with the look and feel of the cards.

Conclusions

Ensuring the integrity of passport cards and BCCs is an essential part of border security requiring continual vigilance to facilitate the travel of those entitled to enter the United States and prevent the entry of those who are not. Preventing the fraudulent use of travel documents requires a combination of well-designed documents with layered security features and an inspection process that utilizes these security features. A well-designed document has limited utility if inspection officers do not utilize the available

[29]Musters are briefings provided daily to CBP officers to provide relevant information, including information about new or updated travel documents and fraud alerts.

[30]The Fraudulent Document Analysis Unit is a part of CBP tasked to remove fraudulent travel documents from circulation and prevent fraudulent use of travel documents to enter the United States.

security features to detect attempts to falsely enter the United States. Although designs for the passport card and the second generation BCC generally meet or exceed standards and guidelines for international travel documents, inclusion of all security features recommended by guidance and standards for international travel documents does not guarantee that the security features are of sufficient quality and are designed to ensure the overall security of the cards. State's development process could be improved to better assess the security of its cards and to fully address problems and issues found during the testing and evaluation of its cards, which could provide greater assurance that State has secure, well-performing documents. We have previously recommended that State periodically assess the security features when redesigning its travel documents. It did not do so when redesigning the passport card. By conducting such an assessment, State potentially could have identified and addressed any vulnerabilities of the passport card's design to resist fraudulent use. State has taken actions to conduct such assessments in future redesigns, which, if effectively implemented, should better position State to identify vulnerabilities in its travel documents' abilities to resist fraud before they can be exploited. Security assessments and testing can provide the added assurance that the cards meet security requirements. However, State did not fully assess or test the security features incorporated on the passport card or the second generation BCC. Although State performed testing and evaluation on prototype passport cards, it did not test and evaluate the final designs for the passport card or second generation BCC, nor did it test and evaluate its recent redesign of the passport card. Further, while State addressed most problems found during its testing, it either did not fully address the issues and recommendations or it did not fully document its decisions for not doing so. More fully conducting testing of the passport card and BCC and addressing identified problems would provide State with a fuller understanding of the overall security and performance of the cards and greater assurance that its cards have been produced with adequate security.

CBP officers at many U.S. ports of entry face time constraints in processing large volumes of people and therefore rely on a few visual and tactile security features of passport cards and BCCs—such as raised printing and the tactile Great Seal—in addition to their interviews, to identify fraudulent use of these documents. To assist officers in the inspection of passport cards and BCCs, CBP deployed systems to its POEs that enable the reading of the RFID chips in the cards and display information about the card holders to the officers during inspection. Further, CBP has deployed fingerprint readers in primary inspection of some of its pedestrian lanes, which could help officers identify imposters

fraudulently using BCCs. State and DHS have taken steps in response to our prior recommendation to improve its training of officers on travel documents. However, the conduct of training without passport card or BCC exemplars at the POEs we visited along the Northern border indicates that improvements are still needed. As State continues to update its travel documents, we continue to believe that State and DHS need to fully implement our prior recommendation to improve training of its officers on new documents prior to their issuance, which includes the provision of exemplars so that they can be used during training to better familiarize officers with the look and feel of the cards.

Recommendations for Executive Action

To ensure the designs for the passport card and BCC physical security features adequately mitigate the risk of fraudulent use, we recommend that the Secretary of State take the following two actions to improve the development process when conducting future redesigns or updates to the passport card or BCC:

- Fully address any issues or problems encountered during testing, including the documentation of reasons for not addressing any of them.
- Fully test or evaluate the security features on the cards as they will be issued, including any significant changes made to the cards' physical construction, security features, or appearance during the development process.

Agency Comments and Our Evaluation

We provided draft copies of this report to the Secretaries of State and Homeland Security for review and comment. We received written comments from State and DHS, which are reprinted in appendices II and III, respectively. We also received technical comments from State and DHS, which we incorporated into the report, as appropriate.

In its comments, State concurred with our recommendations and described actions it is taking to address them. State acknowledges the importance of addressing and documenting issues encountered during testing and that complete testing should be performed on cards whenever significant changes to the physical construction and security features are made.

In its comments, DHS concurred with our finding that sufficient exemplars of new documents should be available for training officer prior to new document issuance. However, DHS commented that, while the report addresses the importance and rate of physically handling travel documents, handling the passport card and BCC is not necessarily the most efficient

means of verifying their validity and the cards can be verified without handling by utilizing RFID technology, Vehicle Primary Client, and other primary systems. We agree that the ability to access cardholder information automatically for the passport card and BCC can help confirm the validity of the cards. Nevertheless, primary inspection is the first and most critical opportunity to detect fraudulent travel documents and to combat this requires inspecting the physical security features, as well as using electronic systems. Both State and DHS's FDL have indicated that physical inspection of the documents is an important part of verifying documents. DHS also commented that, while the use of biometric verification can help identify imposters, operational challenges at busy ports of entry make secondary inspection, where it is currently available, the most efficient location to perform biometric verification. We agree that the use of biometric verification in secondary inspection and in pedestrian lanes enables inspectors to use fingerprint biometrics to verify the identity of the cardholder. However, at vehicle lanes in land border POEs this capability is not available in primary inspection. Furthermore, travelers with BCCs at southern land border ports—the ports where BCC imposter fraud is most significant—are not routinely referred to secondary inspection, where they do have the capability to utilize the fingerprint records for comparison, thus inspectors are not making full use of the biometric information available for BCCs.

As we agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the date of this letter. We will then send copies to interested congressional committees and the Secretaries of State and Homeland Security. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staffs have any questions about this report, please contact me at (202) 512-4499 or barkakatin@gao.gov. Contributors to this report include Richard Hung and Maria Stattel. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report.

Dr. Nabajyoti Barkakati
Chief Technologist
Director, Center for Science,
Technology, and Engineering

Appendix I: Scope and Methodology

To determine how effectively State's development process for the passport card and second generation BCC mitigates the risk of fraudulent use, we interviewed officials from State's Bureau of Consular Affairs, U.S. Customs and Border Protection (CBP), and the Forensic Document Laboratory (FDL) in DHS's U.S. Immigration and Customs Enforcement (ICE). We identified applicable standards and guidelines for international travel cards. We interviewed State and DHS officials on the designs for the security features of the passport card and BCC and assessed them against the applicable standards and guidelines that we identified, including standards and guidelines from DHS, the International Civil Aviation Organization (ICAO), and the Security and Prosperity Partnership (SPP). We also reviewed the results of testing and evaluation of the prototype passport cards and how State and DHS used these results because including all security features recommended by guidance and standards for international travel documents does not guarantee that the security features are of good enough quality and designed well enough together to ensure the overall security of the cards. Testing and evaluation was conducted by the National Institute of Standards and Technology (NIST), FDL, CBP, the Bank of Denmark, and Sandia National Laboratory. Finally, we interviewed officials at the Tucson Passport Center to understand and observe how second generation BCCs are personalized.

To determine how CBP officers use the security features of passport cards and second generation BCCs to prevent fraudulent use at land ports of entry, we interviewed officials from CBP and reviewed CBP policies, procedures, guidance, and training documents regarding the inspection of travelers presenting passport cards and second generation BCCs for the purpose of entry to the United States, including the use of the cards' physical security features and cardholder information retrieved from CBP border inspection systems. We conducted site visits to two POEs along the Southern border and three POEs along the Northern border to interview CBP officials about training and inspection procedures, as well as observe the inspection process of travel documents to understand how CBP officers use the physical security features and DHS database information to verify the eligibility of a traveler presenting a passport card or BCC to enter the United States. To assist in selecting these locations, we devised the following selection criteria:

- RFID Reader in Primary Inspection – First we identified the 41 POEs where CBP planned to install RF readers by June 30, 2009.

- Volume of Passport Cards and Border Crossing Cards – We considered POEs inspecting higher volumes of passport cards and BCCs than other POEs.

- Nearby Ports without RFID Readers – We considered POEs that had nearby POEs without RFID readers within a 2-hour drive for northern POEs and a 3-hour drive for southern POEs.

- Geographic Location – We considered geographic locations ensuring that we include one POE along the border with Mexico and one along the border with Canada.

- Pedestrian Crossing – We considered POEs on the southern border that had pedestrian crossings, as well as vehicle crossings.

In determining potential locations to visit, we considered all of the criteria categories together in making our selections. While the information gathered during these site visits is not generalizable across all land POEs, they did provide insight into the inspection policies and procedures, as well as CBP officer training, for passport cards and second generation BCCs.

We conducted this performance audit from January 2009 to June 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of State

United States Department of State

Chief Financial Officer

Washington, D.C. 20520

MAY 25 2010

Ms. Jacquelyn Williams-Bridgers
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Ms. Williams-Bridgers:

We appreciate the opportunity to review your draft report, "BORDER SECURITY: Improvements in the Department of State's Development Process Could Increase the Security of Passport Cards and Border Crossing Cards," GAO Job Code 460605.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

If you have any questions concerning this response, please contact John Brennan, Senior Advisor, Bureau of Consular Affairs at (202) 647-6370.

Sincerely,

James L. Millette

cc: GAO – Richard Hung
CA – Janice Jacobs
State/OIG – Tracy Burnett

Department of State Comments on GAO Draft Report

BORDER SECURITY: Improvements in the Department of State's Development Process Could Increase the Security of Passport Cards and Border Crossing Cards
(GAO-10-589, GAO Code 460605)

Thank you for the opportunity to comment on your draft report entitled *"Border security: Improvements in the Department of State's Development Process Could Increase the Security of Passport Cards and Border Crossing Cards."*

The Department of State accepts the recommendations of the GAO regarding procedures to be used for redesign and update of the passport card and border crossing card (BCC). We agree it is essential that issues encountered during the testing of a card be addressed and thoroughly documented. We have taken vigorous action to address all substantive concerns during testing or production of the passport card and BCC. We acknowledge that more thorough documentation of these actions would be beneficial. To address this need, the Bureau of Consular Affairs created a permanent position for a Forensic Document Design and Integrity Coordinator, which it filled in September 2009. The Coordinator is a senior official who oversees document design and security issues. The efforts that are the subject of this report preceded creation of this office, which now is regularizing procedures for testing and evaluation of all secure documents produced by the Bureau and will be documenting the results in a manner that will address GAO concerns. We also agree that complete testing of cards is necessary whenever there are significant changes to physical construction and security features and we are committed to regular evaluation of document security throughout the service life of a document. This will be among the priority tasks overseen by the Coordinator.

Concerning steps taken in the redesign of the passport card, we would like to note that changes to the card enhanced a travel document that was already highly secure. The opportunity to make such enhancements arose when it was decided to change the radio frequency identification chip to a chip with a unique tag identifier. All of the security features of the original document and the original artwork designs were retained. The deliberative and decision-making process resulted in a card, which as GAO acknowledges, generally meets standards and guidance for international travel documents and includes numerous layered security features.

Regarding the provision of exemplars for use by other agencies, the Department routinely produces and disseminates exemplars of all new travel documents. Exemplars of the passport card and BCC were provided to requesting agencies prior to the issuance of these cards. We will continue to work closely with other agencies to make sure exemplars are provided in sufficient quantities for training and other purposes.

Appendix III: Comments from the Department of Homeland Security

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

Homeland Security

May 20, 2010

Dr. Nabajyoti Barkakati
Director
Center for Science, Technology, and Engineering
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Dr. Barkakati:

Re: GAO-10-598, *BORDER SECURITY: Improvements in the Department of State's Development Process Could Increase the Security of Passport Cards and Border Crossing Cards*

The Department of Homeland Security (DHS) appreciates the opportunity to review and comment on the U.S. Government Accountability Office's (GAO) draft report referenced above.

The GAO report focuses largely on the security features of the Passport Card and Border Crossing Cards (BCC), and while these are still important, due to technology enhancements implemented under the Western Hemisphere Travel Initiative (WHTI), these documents' validity can be verified electronically. With radio-frequency identification (RFID) technology, the Vehicle Primary Client, other primary systems, and machine readable technology, cards can be verified with no actual handling or inspection of the document by a U.S. Customs and Border Protection (CBP) officer. CBP considers the security features of the cards as an additional means of verifying that the cards are genuine, for cases when systems are not available or discrepancies are identified.

The report mentions the rate at which the cards are actually handled by CBP officers, yet CBP contends that physical handling of the cards is not always necessary and is not the most efficient means of verifying their validity. CBP's electronic systems allow an officer to easily and efficiently identify if a document is valid without handling it.

The largest threat, which the report acknowledges, is that of imposters utilizing genuine documents, not that of fraudulent documents. CBP's electronic systems at primary allow for a better comparison of the document photo on file and biographic information with that of the

traveler, allowing for better identification of imposters. As the report states, CBP has deployed fingerprint scanners to pedestrian lanes to better identify imposters to BCC cards. CBP cannot require U.S. citizens presenting a Passport Card to provide biometrics unless fraud or other violations are suspected, so we must rely on questioning in addition to photo and data comparison in CBP systems. At this time, CBP does not have the capability to verify biometrics in standard vehicle lanes, and given the operational challenges we have at busy ports of entry, secondary inspection is currently the most efficient location to do this. Biometric verification is available at secondary inspection areas.

CBP concurs that sufficient exemplars of new documents should be available for training officers prior to new document issuance.

We appreciate the opportunity to review and comment on this draft report and we look forward to working with you on future homeland security issues.

Sincerely,

Jerald E. Levine
Director
Departmental GAO/OIG Liaison Office