Privacy Impact Assessment Update
for the

United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program

Authentication of e-Passports

August 18, 2006

Contact Point
Steve Yonkers, Privacy Officer
US-VISIT Program Office, DHS
(202) 298-5200

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Abstract

This is an update to previous United States Visitor and Immigrant Status Indicator Technology Program (US-VISIT) privacy impact assessments (PIAs) to address the changes to the port of entry (POE) processing that will result from the deployment of the capability to biometrically compare and authenticate RFID chip-enabled, International Civil Aviation Organization (ICAO)-compliant passports (e-Passports).

Introduction

The US-VISIT Program is a Department of Homeland Security (DHS) integrated, automated biometric entry-exit system that records the arrival and departure of certain aliens (defined as any person not a citizen or national of the United States (U.S.)); conducts certain terrorist, criminal, and immigration violation checks on aliens; and compares biometric identifiers to those collected on previous encounters to verify identity. US-VISIT has published a number of privacy impact assessments (PIAs) that describe how the Program operates and detail any privacy impacts and mitigations.[1] This PIA update reflects changes to the port of entry (POE) processing that will result from deployment of the capability to biometrically compare and authenticate RFID chip-enabled, ICAO-compliant passports (e-Passports). This PIA does not cover risks associated with the actual e-Passports. Any issues relating to the design or security and privacy controls employed will be the responsibility of the country issuing the passport. For example, in the case of U.S. issued e-Passports, the Department of State (DOS) is assessing the risks presented by the passports themselves and determining how best to mitigate them. This PIA also covers how the captured information will be handled by DHS if a U.S. issued e-Passport is processed, during the normal course of business, by an e-Passport reader.

This new capability is part of the DHS implementation of the requirements of the Enhanced Border Security and Visa Entry Reform Act of 2002, as amended (Border Security Act). The Border Security Act requires that: Visa Waiver Program (VWP) countries implement programs to issue machine readable, tamper resistant, ICAO compliant passports that incorporate biometrics; individuals applying for admission under the VWP program present a document meeting the standards identified above; and DHS deploy equipment and software necessary to biometrically compare and authenticate these documents. DHS has interpreted this statute to require: applicants for admission under VWP to present e-Passports as of October 26, 2006; and DHS deployment

[1] US-VISIT PIA, Increment 1, December 18, 2003; US-VISIT PIA, Increment 2, September 14, 2004; US-VISIT PIA, International Live Test, June 15, 2005; US-VISIT PIA, Exit, July 1, 2005; US-VISIT PIA, Update, December 22, 2005; US-VISIT PIA, Update, March 14, 2006. All PIAs are available from the DHS Privacy Office website, www.dhs.gov/dhspublic/interapp/editorial/editorial_0511.xml

and use of e-Passport readers as of the same date. In addition, DOS is beginning the process of issuing ICAO-compliant e-Passport to United States Citizens (USC).

Just as with machine-readable passports currently used, the e-Passport will contain all of the biographic data that is currently included on the passport's document information page as text and a photograph and, for biographic data, in the passport's machine readable zone (MRZ). In addition, the e-Passport will also contain a radio frequency identification (RFID) chip that will hold a copy of the biographic information from the passport's document information page and a digital copy of the passport holder's photograph. In order to support this new type of passport, DHS acquired reader technology capable of reading and authenticating these new travel documents, as well as continuing to read the current machine readable passports or other machine-readable travel documents. The elements collected by DHS from the machine readable zone (MRZ) of a passport, both currently, and with the new e-Passport readers, include: document type; issuing country code; document bearer name; document number; bearer nationality; date of birth: gender; and, document expiration date.

Current Inspections Process for Processing Passports

Currently, when a foreign traveler, in-scope for the US-VISIT program, enters the Primary inspection area and presents a passport, the Customs and Border Protection (CBP) Officer scans the presented documentation and begins the interview process. The officer uses a reader to access the biographic data contained in the Machine Readable Zone (MRZ) of the passport. Upon reading the passport, the most recent facial image collected is recalled from DHS systems and displayed (if available). The officer then compares the photograph that is displayed on the workstation screen with the traveler presenting the document, and with the photograph printed in the travel document.

The officer may decide to refer the visitor to secondary inspection for further scrutiny, based on the interview results, as well as information that has been retrieved from the automated query, and/or presented documentation. Once the Secondary officer is presented with the results of the various systems checks, the officer completes the interview with the traveler, returns the traveler's documentation, updates the data displayed on the screen, and admits the traveler to the U.S. or takes other action as appropriate.

Updated Inspections Process for Processing e-Passports

Once the new readers are deployed to the POEs, the foreign traveler, in-scope for the US-VISIT program, will enter the Primary inspection area and present an e-Passport. The CBP Officer will use the new, full-page, integrated reader to access the data in the MRZ on the e-Passport, and to open the RFID chip on the e-Passport. The officer will now have the benefit of using four avenues for document validation: the photograph and biographic information in the physical passport; the visitor who is physically being interviewed; the RFID chip-specific, digitally encoded photograph that will be stored in the RFID chip on the e-Passport; and information from previous encounters

(where present). The RFID chip on the e-Passport contains the same biographic information stored in the MRZ except for the addition of the bearer's digitized photograph.

As soon as the e-Passport is successfully opened and scanned, the e-Passport reader performs an automated comparison of the biographic data on the contactless integrated RFID chip and the biographic data printed in the MRZ to confirm that the information on the e-Passport is valid and has not been changed or subjected to tampering. The digitized photograph that has been retrieved from the RFID chip will be displayed to the officer for comparison with the photograph that is printed in the passport, and with the traveler presenting the document, providing assurance that the person presenting the e-Passport is the same person to whom it was issued.

The digital photograph contained on the e-Passport RFID chip will be collected and retained in DHS systems. Upon subsequent entries into the United States after reading the e-Passport, the system will compare the electronic security information surrounding the digitized photograph from the RFID chip with those stored in DHS systems. This will allow the officer to look at the system comparison of the security features, the retrieved photograph from the RFID chip, and the traveler being processed, thus improving the officer's ability to validate that the document is a legitimate travel document, and that the person being processed is not an imposter. This new approach improves DHS' ability to confirm both the authenticity and legitimacy of the document, and its linkage to the traveler.

United States Citizens (USC) are processed through specific lanes at POEs that will not be equipped with the e-Passport reader technology. However, between August 22, 2006 and October 26, 2006, if a USC carrying an e-Passport uses a lane equipped with an e-Passport reader, the digitized photograph from the e-Passport will be automatically read and stored in a CBP system. The photograph would then be deleted by CBP as part of its data integrity processing on a regular basis. By October 26, 2006, a software change will be implemented to prevent the e-Passport reader from automatically storing USC digitized photographs. This software change will ensure that USCs who use the e-Passport lanes will not have their digitized photographs stored or retained. In the future, should DHS choose to process USCs through e-Passport lanes and/or retain their digitized photographs, DHS will first provide notice through publishing a new PIA.

In preparation for the October 26, 2006 deployment of e-Passport reading capability at U.S. POEs, DHS evaluated the performance, both technically and operationally, of the e-Passport reader solutions during an International Live Test. The PIA for Phase I of the International Live Test was published in the Federal Register on June 15, 2005. Updates were made to this PIA on December 12, 2005, and on March 15, 2006. This current PIA describes the implementation of the e-Passport biometric comparison and authentication capability that will occur at the U.S. POEs beginning on or about August 22, 2006 to meet the October 26, 2006 deadline.

Section 1.0
Information collected and maintained

The following questions are intended to define the scope of the information requested as well as the reasons for its collection as part of the system, rule, and/or technology being developed.

1.1 What information is to be collected?

DHS is currently collecting the following information from the passport's document information page by reading the MRZ:

Document Type	Bearer Nationality
Issuing Country Code	Date of Birth
Document Bearer Name	Gender
Document Number	Document Expiration Date

With the new reader, DHS will now collect all of the above passport information as well as a copy of the passport holder's photograph from e-Passports RFID chips. DHS will collect and store both the MRZ data elements and the photograph from the RFID chip from e-Passports.

1.2 From whom is information collected?

E-Passport information will be collected from all in-scope US-VISIT travelers entering the United States. USCs who use a lane equipped with an e-Passport reader between August 22, 2006 and October 26, 2006 will also have their e-Passport information collected, but the information will be deleted from the system.

1.3 How is information collected?

The MRZ data will be collected in the same manner as it is currently collected today – through a scan. In addition, the digital photograph will be extracted from the RFID chip. The MRZ information may also be accessed through the RFID chip to compare with the MRZ information contained on the data page of the passport.

1.4 Why is the information being collected?

The only new information being collected is the digital photograph. The digital photo is collected as an additional level of security to ensure that there is a match between the digitized photo from the e-Passport, any previously collected digital photo, if applicable, and the physical representation on the passport data page. If there is any question as to the validity of the digital photo, a previously collected digital photo can be pulled up and compared to the current digital photo. In addition, the photo is used to help verify traveler's identity to determine that the person presenting the document is the same person to whom the government issued it. In addition, DHS will conduct watchlist checks to determine whether individuals are admissible, have violated the terms of their admission, should be prevented from obtaining an immigration benefit, or should be removed from the country.

1.5 What specific legal authorities/arrangements/agreements define the collection of information?

The Border Security Act requires that: Visa Waiver Program (VWP) countries implement programs to issue machine readable, tamper resistant, ICAO compliant passports that incorporate biometrics; individuals applying for admission under the VWP program present a document meeting the standards identified above; and DHS deploy equipment and software necessary to biometrically compare and authenticate these documents. DHS has interpreted this statute to require: applicants for admission under VWP to present e-Passports as of October 26, 2006; and DHS deployment and use of e-Passport readers as of the same date. These changes are being put in place to strengthen the assurance that travel documents are authentic, thereby enhancing national security.

1.6 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

The digitized photograph from the e-Passport RFID chip is the only new data element being collected during the e-Passport reader processing. The photograph itself was previously, and will continue to be, available on the data page of the e-Passport for viewing by the officer. However, the collection and storage of the digitized photograph will assist the officer in validating the authenticity of the document on subsequent uses of that document. It will provide assurance that the document was not altered or counterfeited, and will give the officer four different avenues for determining whether the traveler is an imposter.

Section 2.0
Uses of the system and the information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

Other than travel document verification, there is no change to the uses of traveler information that is being collected using the new processes for e-Passports. DHS uses the information that is collected and maintained by US-VISIT to carry out its assigned national security, law enforcement, immigration, intelligence and other DHS mission-related functions. Through the enhancement and integration of its processes and data, DHS is able to ensure the entry of legitimate travelers; identify, investigate, apprehend and/or remove individuals unlawfully entering or present in the United States beyond the lawful limitations of their visit; and prevent the entry of inadmissible individuals. US-VISIT will also help DHS prevent covered individuals from obtaining immigration benefits to which they are not entitled.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as data mining)?

US-VISIT does not currently use data mining technology within the direct program environment. However, US-VISIT shares biometric and biographic data with DHS components and other federal agencies that make use of data mining for the purposes of both investigative and intelligence gathering purposes. See Sections 4 and 5 regarding information collection and sharing.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Each MRZ of an e-Passport is queried upon entry into the United States. CBP uses software to validate that there are no errors in the MRZ and performs all biographic queries that are necessary for the inspection process. If an MRZ error occurs, the system will notify the officer and the officer will manually enter the biographic information for a query. Basic Access Control (BAC) enabled e-Passports require DHS readers to read the second line of the MRZ in order to access the chip information. If the MRZ does not read properly on a BAC enabled e-Passport, the RFID chip will not open, and the officer will be alerted that there is a problem with the MRZ or with the RFID chip. The officer will have to manually enter the biographic information. An error in the MRZ read may also alert the officer to an alteration in the document, or encourage additional

questioning by the officer to determine whether the traveler is an imposter or otherwise a subject of interest.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above-described uses.

US-VISIT uses a quality assurance process to identify any errors in properly matching individuals with relevant records, and vice versa, and to implement risk mitigation as needed, e.g., special checks targeted at specific data elements exhibiting a statistically significant tendency to cause matching errors. US-VISIT's redress process provides multiple points at which inaccurate data can be corrected, beyond the on-the-spot corrections at POEs. Redress is discussed more fully in Section 7.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What is the retention period for the data in the system?

The information captured from the e-Passport RFID chip, including the digitized photograph, is retained for up to 75 years, the same as for information previously collected solely by the MRZ read.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

The retention schedule is awaiting NARA approval.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

The processing of e-Passports involves multiple systems with varying retention periods based on their business needs and missions. US-VISIT is working with NARA to develop a retention policy that can be uniformly applied to appropriate component systems and that will address the needs of

US-VISIT stakeholders. This process includes conducting interviews with both operational and records experts affiliated with each stakeholder to accurately capture retention requirements.

Section 4.0
Internal sharing and disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organizations is the information shared?

The internal organizations receiving this data will not change. Passport data continues to be shared throughout DHS for relevant national security, law enforcement, immigration, intelligence and other DHS mission-related purposes. This data is used by CBP, Immigration and Customs Enforcement (ICE), and United States Citizenship and Immigration Services (USCIS). The only new information collected is the digitized photograph from the e-Passport RFID chip. DHS personnel carrying out immigration and border management activities will potentially have access to this data, and will have to go through appropriate channels to gain access.

4.2 For each organization, what information is shared and for what purpose?

Employees of DHS components, including CBP, ICE, and USCIS access the personal information collected from the e-Passports for DHS national security, law enforcement, immigration, intelligence and other DHS mission-related purposes.

4.3 How is the information transmitted or disclosed?

The data is electronically transmitted between the various DHS organizations. All data transmissions are conducted within the DHS networks, and are secured by one or more organizational units within DHS.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

There is no change to internal data sharing of information. DHS internal data sharing of e-Passport information is required to comply with statutory requirements for DHS national security, law enforcement, immigration, intelligence and other DHS mission-related purposes. Any sharing of information, whether internal or external, increases the potential for compromising that

information and creates new opportunities for misuse. DHS mitigates these vulnerabilities by working closely with the sharing organizations to develop secure standard operating procedures for sharing this information. These procedures are documented in sharing agreements. Only those individuals with both the authority and need to know are provided access. Furthermore, the information and access is limited using role based access controls or a limited technical interface. In all cases of sharing internal to DHS, all organizations are required to comply with the Department's security policies and procedures. Each database has a user id and a password that has to be changed every ninety days. Logs are kept of who accesses what system(s) and what information is accessed. These logs are checked periodically. In most cases, these organizations have gone beyond the Department's requirements and have instituted even greater security policies and procedures.

Section 5.0
External sharing and disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS, which includes Federal, state and local government, and the private sector.

5.1 With which external organizations is the information shared?

DHS shares, and will continue to share, e-Passport data back to DOS as well as to the Department of Justice (DOJ), and other Federal, state, local, foreign, and tribal agencies lawfully engaged in collection and processing of biometric and limited biographic information for DHS national security, law enforcement, immigration, intelligence and other DHS mission-related functions.

5.2 What information is shared and for what purpose?

DHS shares both the e-Passport biometric and biographic data with the following external entities:

- DOS to support visa decision making, and
- DOJ/Federal Bureau of Investigation (FBI) for the purpose of national security and/or criminal investigations.

Additionally, DHS may also share information with other agencies at the Federal, state, local, foreign, or tribal level who are lawfully engaged in the collection and processing of biometric and limited biographic information for DHS national security, law enforcement, immigration, intelligence and other DHS mission-related functions, or in accordance with the sharing agreement that exists between DHS and the particular agency. Any disclosure by DHS must be compatible with the purpose(s) for which the information was collected. Additionally, any non-DHS agency

granted direct access to this information must sign a data sharing agreement that will govern protection and usage of the information.

5.3 How is the information transmitted or disclosed?

Information is transmitted or disclosed to external organizations in one or more of the following ways:

- DHS directly transmits e-Passport information to other agencies' systems through limited connections;
- External agencies directly access DHS system with a user access account and limited access, and/or
- External agencies receive e-Passport information via secure transfer on encrypted portable media, (e.g., CDs or tapes), when there is no direct connection between systems.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

DHS has entered into MOUs or other agreements for sharing of e-Passport data with non-DHS organizations. These agreements provide the conditions of sharing or disclosure, including governing the protection and use of the information. The appropriate/relevant organizational entities that receive access currently have data sharing agreements in place with Federal, state, and local agencies for each system.

5.5 How is the shared information secured by the recipient?

External connections must be documented and approved with each party's signature in an interagency security agreement (ISA) that outlines controls in place to protect the confidentiality, integrity, and availability of information being shared or processed. Organizations with which DHS shares information must agree to maintain reasonable physical, electronic, and procedural safeguards to appropriately protect the shared information. Furthermore, recipient organizations must notify DHS as soon as reasonably practicable, but not later than within 24 hours, after they become aware of any breach of security of interconnected systems or unauthorized use or disclosure of personal information.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

All information users must complete security and privacy training.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

The existing sharing agreements provide for controls on what information is shared, how it is shared, and the use and retention of the information once the information is shared. The changes for the processing of e-Passports will require no modifications to external sharing agreements, as there are no changes to the sharing of information.

Section 6.0
Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

The e-Passport reader solution will be deployed to POEs beginning on August 22, 2006. Major POEs processing VWP travelers will have the capability by October 26, 2006. Notice is provided by means of the publication of this PIA on the DHS website and in the Federal Register. Signage indicating which lanes process e-Passports will be installed at POEs. Countries are responsible for informing their citizens about the e-Passports.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

There is no change to the opportunity and/or right to decline to provide information as a result of this change in US-VISIT processing. The presentation of a passport is required for admission into the U.S. Individuals who decline to present their passport, whether it is an e-Passport or not, could be denied entry.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

The collected information is used only for DHS national security, law enforcement, immigration, intelligence and other DHS mission-related purposes. Individuals exercise a choice when they come to the United States and must supply the requested information in order to be admitted entry.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

DHS has made a strong commitment to ensure that the privacy of all visitors to the U.S. is respected, and to respond to individual concerns raised about the collection of the required information. Further, the DHS Chief Privacy Officer, who serves as the administrative appellate review authority for all individual complaints and concerns about the program, exercises comprehensive oversight of all phases of the program to ensure that privacy concerns are respected throughout implementation.

US-VISIT has posted entry requirements on its web site and at airport locations, and disseminates entry requirements through consular offices overseas. US-VISIT continues to communicate through both diplomatic channels and public outreach all e-Passport requirements and e-Passport reader technology capabilities. Since the first International Live Test was conducted in Los Angeles, the US-VISIT Outreach department has helped the program to actively communicate to both foreign and domestic stakeholders. US-VISIT will continue to outline the benefits associated with utilizing new technology, and how that technology affects the traveling public. However, it continues to be the responsibility of travelers to take proactive steps to identify the U.S. entry requirements before they travel.

Section 7.0
Individual Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures which allow individuals to gain access to their own information?

US-VISIT will continue its current redress process of providing individuals an opportunity to have access to their own information and have their information reviewed and corrected. Individuals are allowed to have their records reviewed for accuracy at the POE. This is the first opportunity an individual is allowed access to his or her own information. Thereafter, individuals must request information directly through the Redress process.

7.2 What are the procedures for correcting erroneous information?

In most cases, if there is a need for correction to the passport, the individual would go to the passport issuing authority. If the reader did not correctly capture the information that is on the RFID chip in the e-Passport, the officer may correct it. If additional redress is required for information captured specifically for the US-VISIT program, either the officer sends a data correction request to US-VISIT, or an individual may request that the US-VISIT Privacy Officer review his or her records.

7.3 How are individuals notified of the procedures for correcting their information?

The US-VISIT website, www.dhs.gov/us-visit, provides procedures and a Redress Request Form for correcting information. If individuals do not have access to the US-VISIT website, they may request a copy of the Redress Request Form and instructions directly from the Privacy Officer by calling (202) 298-5200. The US-VISIT Privacy Office has set a goal of processing redress requests within 20 business days based upon the number of requests. If an individual is not satisfied with the response received from US-VISIT, an individual can appeal his or her case to the DHS Chief Privacy Officer, who will conduct a review and provide final adjudication on the matter.

7.4 If no redress is provided, are alternatives are available?

Redress opportunities are provided through the US-VISIT website: www.dhs.gov/us-visit.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, what procedural rights are provided and, if access, correction and redress rights are not provided please explain why not.

US-VISIT will continue its current redress process of providing individuals an opportunity to have access to their own information and have their information reviewed and corrected. However,

many of the redress requests that might arise around the collection of information as described for this PIA would more properly be addressed to other organizations such as DOS, CBP, or the passport issuing authority for their passport. When practicable, these requests will be forwarded to the correct organization, or the requester will be notified of the appropriate agency for the request.

Section 8.0
Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

There are no changes to the user groups as a result of this change. The primary user groups having access to the e-Passport readers are CBP officers. Other user groups might include ICE agents, USCIS officers, and DOS consular officers. Users from other external agencies have limited access that is described by the sharing agreement between that agency and US-VISIT. Other groups have limited access, including developers, workstation attendants, program managers, and information technology (IT) staff. These limits may be based on time, such as developers processing existing data as systems are developed and implemented, or the limit may be based on need, such as workstation attendants who will only have access to the information necessary to assist covered travelers as part of Exit. Managers and IT staff have limited access based on their specific roles and responsibilities.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Contractors are given access based on their assigned roles and responsibilities in accordance with DHS policy. Access to DHS systems is managed through a logon and password issuance control process. Copies of the contracts have been submitted to the DHS Privacy Office.

8.3 Does the system use "roles" to assign privileges to users of the system?

Access to the e-Passport readers and the associated automated systems will be assigned based on the specific roles of the users. Roles are created for each level of access required for individuals to perform their job functions. Examples of roles include basic user, system administrator, system auditor, and system manager.

8.4 What procedures are in place to determine which users may access the system and are they documented?

CBP has documented standard operating procedures to determine which users may access the e-Passport readers and associated systems supporting their use. US-VISIT has procedures for determining who may gain access to US-VISIT information and the extent of that access. The minimum requirements for access to US-VISIT information is documented in DHS and US-VISIT security documentation, and includes a DHS security clearance, security and privacy training, and need based on job responsibility. Similar approaches and documentation are used by CBP.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Access roles are assigned by the system manager for each component and are reviewed regularly to ensure that users have the appropriate access. Individuals who no longer require access are immediately removed from the access list. Access is audited and the audit logs are reviewed on a regular basis.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

US-VISIT and CBP secure information - and the systems on which that information resides - by complying with the requirements of DHS information technology security policy, particularly the *DHS Information Technology (IT) Security Program Handbook for Sensitive Systems (Attachment A to DHS Management Directive 4300.1)*. This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules, which are applied to component systems, communications between component systems, and at all interfaces between component systems and external systems.

One aspect of the DHS comprehensive program to provide information security involves the establishment of strict rules of behavior for each major application, including those used by US-VISIT and CBP. The security policy also requires that all users be adequately trained regarding the security of their systems. The program also requires a periodic assessment of physical, technical, and administrative controls to enhance accountability and data integrity. All system users must complete security training. External connections must be documented and approved with both parties signature in an ISA, which outlines controls in place to protect the confidentiality, integrity, and availability of information being shared or processed.

US-VISIT is also in the process of developing a public key directory (PKD), which will be used to validate the authenticity of the RFID chip within the e-Passport and assure the chain-of-trust between the e-Passport issuing authorities and the e-Passport itself. PKD is a higher level technical solution for identity verification and will provide increased protection above and beyond BAC. This change to the current process is required to strengthen the assurance that travel documents are authentic, thereby enhancing national security.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

US-VISIT has developed a privacy-training program that is given to all new US-VISIT employees and contractors. This training is also provided to individuals in other organizations who have access to the US-VISIT information. The privacy training provides a thorough introduction to the US-VISIT Privacy Policy, Privacy Principles, and Privacy Rules of Behavior. It describes both what is required of individuals handling personal information and the consequences of failing to comply with these requirements.

CBP officers who operate the e-Passport readers will have received extensive formal training in the areas of privacy and security. This training covers appropriate handling and protection of information during face-to-face interactions with travelers and for the handling of sensitive documents. The training is reinforced every twelve months and the officers must have completed security and privacy training as a part of the training on all new technology.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

The data is secured in accordance with DHS and national-level security requirements, including the Federal Information Security Management Act (FISMA) requirements. The readers are considered to be an enhancement to CBP's Treasury Enforcement Computer System (TECS) and will be covered under its Certification and Accreditation which has an existing authority to operate that expires January 3, 2009.

While there is a possibility of eavesdropping with virtually any technical solution, this risk is considered minimal because of technical controls to ensure security of the e-Passport readers and the fact that the readers will only be located in the designated Federal Inspection Service (FIS) area. The FIS area is a controlled area that is only accessible to those people who have the appropriate clearances and badge to enter the FIS area. Usually it is controlled electronically, and persons entering the FIS area have to swipe their badge to gain access to the area. The doors to the FIS area are alarmed in and out of the area to deter the entry of non-authorized persons into the area. If

someone attempts to enter or exit the area the alarms sound and CBP automatically goes to the door where the alarm occurred.

In addition to the normal airport or seaport badge that is required, CBP also requires a special seal to be placed and displayed on the badge for employees that work in the FIS area. This seal signifies that the person has been vetted by CBP and is authorized access to these areas for official business only. CBP requires that all personnel including officers working in the FIS area display the badge at all times. Those who are not in compliance are questioned and challenged and are at a minimum escorted out of the area. Those persons who require admission into the area, but are not in possession of a badge are escorted by a CBP official at all times.

The majority of individuals in the FIS area are those international travelers and airline crew who are being processed for entry into the United States. In general, arriving passengers to the United States must get to the FIS area through a sterile corridor that is segregated from the domestic passenger environment. Rovers from CBP are constantly moving throughout the FIS area and the jet ways to look for suspicious people or activities.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

The e-Passport readers will undergo security testing and evaluation as a part of the update to the TECS Certification and Accreditation package. Generally, the readers are secured based on their presence in the CBP controlled area that has severely restricted access. The equipment used in the FIS area is controlled by CBP/Office of Information Technology (CBP/OIT). All equipment is installed at the ports of entry by CBP/OIT. Therefore, unauthorized equipment would be extremely difficult to bring into the secured environment. Rovers from CBP are constantly moving throughout the FIS area and the jet ways to look for suspicious people or activities.

US-VISIT is also in the process of developing a public key directory (PKD), which will be used to validate the authenticity of the RFID chip within the e-Passport and assure the chain-of-trust between the e-Passport issuing authorities and the e-Passport itself. This capability will assist in ensuring that passports have not been tampered with.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Was the system built from the ground up or purchased and installed?

The e-Passport readers were purchased and installed. US-VISIT has developed its technical systems and elements since initial inception by combining and customizing commercially available technologies.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Data integrity, privacy, and security were all significant factors that influenced the development of the e-Passport reader solution. This included extensive testing by the National Institute for Standards and Technology (NIST) of the reader. As previously noted, there has been some difficulty with reading data from non-ICAO-compliant e-Passport RFID chips. US-VISIT continues to try to make the readers capable of all appropriate reads and to continue to encourage all countries adopting e-Passports to use ICAO standards.

US-VISIT uses a privacy risk management process based on information life cycle analysis and fair information principles. Technical and programmatic design choices are informed by this approach, which analyzes proposed changes in terms of their life-cycle processes—collection, use and disclosure, processing, and retention and destruction—and the potential they may create for noncompliance with relevant statutes or regulations (the Privacy Act in particular) or for violations of fair information principles. When analysis determines that privacy risks may exist, either alternative design choices or appropriate technical, physical, and/or procedural mitigations are developed.

9.3 What design choices were made to enhance privacy?

Congress mandated the use of machine-readable, tamper-resistant, biometric-enabled travel and entry documents. US-VISIT has made protecting the personal information of travelers one of its primary goals and ensured that privacy was considered throughout the reader design and development process before, during and after technology testing. BAC-enabled e-Passports require DHS readers to read the second line of the MRZ in order to access the chip information. If the MRZ does not read properly on a BAC enabled e-Passport, the RFID chip will not open, and the officer will be alerted that there is a problem with the MRZ and opening the RFID chip. In each instance, the officer will be alerted that there was an error with the MRZ data. This may also alert the officer to an alteration in the document, or encourage additional questioning by the officer to determine whether the traveler is an imposter or otherwise a subject of interest. The US-VISIT privacy and information security teams worked closely together to review and mitigate the risk of

data exposure or interception during the reading of the e-Passport during the CBP inspections process.

9.4 Privacy Impact Analysis: Given the above choices regarding technology, what privacy impacts were considered and how were they resolved?

The congressional mandate to use machine-readable, tamper-resistant, biometric-enabled, ICAO compliant travel and entry documents dictated some of the reader capabilities and choices. However, no high-level and only a few low-level risks were identified. For example, there is a low-level risk for data integrity problems because of non-compliant e-Passports. In addition, while privacy risks associated with the e-Passports themselves are beyond the scope of this PIA, US-VISIT staff has actively encouraged other nations to follow the ICAO standards to facilitate entry and exit and provide information protection. Ultimately any e-Passport privacy risks would be addressed by the passport issuing authorities. Additionally, there is a low-level risk of eavesdropping while the e-Passport is being read, however because the readers are located in the CBP controlled area the opportunity to eavesdrop is minimized.

Conclusion

Although the adoption of the full business process of issuing, reading, and processing e-Passports has implications for the DOS, CBP, US-VISIT, as well as other nations, the addition of the capability to read and authenticate e-Passports at U.S. POEs creates minimal privacy risk to the holders of e-Passports. The low-level risk of eavesdropping during the e-Passport reading process is minimized by the physical and operational controls that exist in the CBP inspections area. As the reader technology matures US-VISIT will be looking to enhance the readers and reading process with the capability to further minimize eavesdropping.

Responsible Officials

Steve Yonkers, US-VISIT Privacy Officer
Department of Homeland Security

Approval Signature Page

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security