Privacy Impact Assessment
for the

Air Entry/Exit Re-engineering (AEER) Project

DHS/S&T/PIA-028

May 28, 2014

Contact Point
Robert Burns
APEX Program Manager
Science and Technology Directorate
(202) 254-6104

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The United States Congress mandated that the Secretary of Homeland Security implement a biometric verification system to monitor the arrival and departure of foreign nationals entering and departing the country. The Secretary in turn directed the U.S. Customs and Border Protection and the Science and Technology Directorate to test various biometric verification systems for effectiveness and efficiency. This privacy impact assessment addresses the privacy risks and mitigation strategies associated with the testing phase of the Air Entry/Exit Re-Engineering Project.

Introduction

Several federal statutes require the Department of Homeland Security (DHS) to develop and implement a full biometric entry and exit system:

1) the Illegal Immigration Reform and Immigrant Responsibility Act of 1996;[1]
2) the Immigration and Naturalization Service Data Management Improvement Act of 2000;[2]
3) the Visa Waiver Permanent Program Act;[3]
4) the Enhanced Border Security and Visa Entry Reform Act of 2002;[4] and
5) the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.[5]

The DHS Science & Technology Directorate (S&T) and U.S. Customs and Border Protection (CBP) components initiated the Air Entry/Exit Re-Engineering (AEER) Project to meet these mandates in these statutes.

The initial objective of this project is to test, evaluate, and develop options to implement biometric entry and exit options that will improve screening and verifying the identities of foreign nationals entering or exiting the United States through U.S. airports.

S&T and CBP are developing, testing, and evaluating four potential solutions. The testing phase is evaluating the use of fingerprint data, iris image data, and facial recognition technologies under simulated airport conditions. Fingerprint recognition technology uses digital imaging and compares two instances of friction ridge skin impressions from a person's fingers. Iris image data uses digital images and analyzes the random pattern of the iris, a muscle that

[1] P.L. No. 104–208, Title I, Subtitle A, Sec. 104 (http://www.gpo.gov/fdsys/pkg/PLAW-104publ208/html/PLAW-104publ208.htm).
[2] P.L. No. 106–205, Sec. 110 (http://www.gpo.gov/fdsys/pkg/PLAW-106publ215/pdf/PLAW-106publ215.pdf).
[3] P.L. No. 106–396, Sec 205 (http://www.gpo.gov/fdsys/pkg/PLAW-106publ396/pdf/PLAW-106publ396.pdf).
[4] P.L. No. 107–173, Title III, Sec. 303 [8 U.S.C. 1701 et seq.] (http://www.gpo.gov/fdsys/pkg/PLAW-107publ173/pdf/PLAW-107publ173.pdf).
[5] P.L. No. 107–56, Title X, Sec. 1008 (http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf).

forms the colored portion of the eye. Facial recognition technologies recognize a person by comparing two or more digital face images. These technologies and associated processes are being evaluated for viability, feasibility, and potential operational effectiveness based on ease-of-use, time requirements, accuracy, and performance. Privacy impact is one of the factors that will contribute to the decision to roll out a technology.

There are three phases to the project; the initial phase seeks to determine which technologies are most accurate. The second phase will test the processes and technologies at a U.S. airport, and the third phase will involve pre-operational testing and implementation at multiple U.S. airports. Additional details about the second and third phases will be provided in future privacy impact assessments. The overall decision to implement a technology will consider how well the technology is received by the traveling public, airlines, flight crews, airport authorities, and government authorities, along with the other factors listed above.

Volunteer Participants

1. Information Collected.

S&T is testing these technologies with volunteers in a controlled laboratory that resembles an airport environment. S&T is contracting with a non-governmental, third-party organization. The contractor identifies and selects volunteer participants, collects basic contact and demographic information from the volunteers. The contractor also conducts interviews with the volunteers and informs them of the test and evaluation activities. The contractor does not provide DHS with information that discloses the actual identities of the volunteers. The contractor recruits volunteer participants through newspaper advertisements, online advertisements, pamphlets, and flyers. An independent Institutional Review Board (IRB)[6] evaluated this project and has not identified any physical or psychosocial risks to the volunteer participants.

The contractor collects medical information to determine whether a volunteer can safely participate in the study, including information about whether a volunteer has a significant medical, psychiatric, or substance abuse condition that would likely affect his or her ability to participate in the study. The study also requests information about current medications the person takes to help determine if certain sensors do not work with certain people. Other questions asked include whether a volunteer wears glasses or contact lenses or has had a significant injury to the face, eyes, or fingers. This information is critical to test and evaluate the most effective biometric technology. If the testing phase shows that a technology does not work on a significant sector of the traveling population because of a common medical condition, that will factor in to future decisions about whether that technology is operationally viable.

[6] An Institutional Review Board (IRB), also known as an independent ethics committee or ethical review board, is a committee formally designated to approve, monitor, and review biomedical and behavioral research involving humans.

Volunteers sign informed consent agreements acknowledging that they understand the test activities, that personally identifiable information (PII) is being collected, and how the information will be used. After the informed consent agreements are signed, the contractor collects biometric data (fingerprint, iris scan, and photograph for facial recognition) from the volunteers and enrolls the data in a database used only for test and evaluation purposes.

2. Anonymization Mechanisms.

The contractor assigns anonymized user identification credentials to each volunteer. The credentials include pseudonyms, tokens representing passports, and travel documents using the assigned pseudonyms. DHS only receives aggregated data from the contractor, such as the False Match Rate (FMR),[7] False Non-Match Rate (FNMR),[8] Failure to Acquire Rate (FTAR),[9] False Rejection Rate (FRR),[10] transaction time, and throughput analysis. The contractor also provides aggregated data about gender, age, nation of origin, and whether English is the volunteer's primary language.

3. Testing Facilities and Environment.

S&T is primarily interested in testing how well the biometric sensor suites work and what effect new processes will have on passenger and crowd flows. The actual identities of the volunteers are not important to the study. The actual identities of the passengers will not be relevant until CBP and S&T move into a pre-operational testing phase at a U.S. airport, involving actual international travelers. This PIA will be updated or a new PIA will be written for the field trial and operational implementation phases.

S&T and CBP are conducting testing at a warehouse that has been renovated to simulate an airport. Several different scenarios are being tested within the facility:

1) **Test Scenario – Boarding Gate Capture Solution:** A volunteer participant checks-in for his or her flight and acquires his or her paper or e-boarding pass.
    a. The volunteer makes his or her way from check-in to the boarding gate.
    b. The volunteer scans his or her boarding pass barcode using automated gates with integrated barcode readers.
    c. The boarding pass scan is required to determine whether or not a passenger is required to provide biometric data.

[7] Percentage of time an imposter user's biometric is accepted and treated as a genuine match.
[8] Percentage of time a genuine user's biometric is rejected and treated as an imposter match.
[9] Percentage of time a biometric feature was not able to be successfully collected due to an error caused by the human user, environment, or the biometric capture device.
[10] Percentage of time a user's biometric is rejected.

d. Displays contained in the gate or signage instructs the participant to provide a fingerprint or look at a specific point while a camera captures high-quality iris and face image(s).

e. The captured biometric is matched to the volunteer's enrolled biometric information that was previously collected.

f. The biometric information is associated with the volunteer's assigned biographic information, and retrieved through the boarding pass scan.

g. The participant proceeds through the simulated boarding gate.

2) **Test Scenario – Centralized Capture Solution:** Like the boarding gate capture concept, the centralized capture concept begins when a volunteer participant checks-in for his or her flight and acquires either a paper or e-boarding pass.

a. The volunteer proceeds to a centralized area equipped with multiple biographic/biometric capture devices preceding the departure area.

b. The volunteer scans his or her boarding pass barcode or travel document using automated gates with integrated barcode readers.

c. The boarding pass/travel document indicates whether the volunteer is required to provide biometric information.[11]

d. Displays contained in the gate or signage instructs the participant to provide a fingerprint or look at a specific point while a camera captures high-quality iris and face image(s).

e. The captured biometric is matched to the volunteer's enrolled biometric information that was previously collected after the interview process and during the biometric data enrollment process.

f. The collected biometric information is associated with the volunteer's assigned biographic information and retrieved through the boarding pass scan.

g. The participant proceeds to his or her boarding gate.

h. The volunteer's biometric is matched against the biometric entry record.

[11] In this instance a token such as a travel document/boarding pass given to the volunteer will include information that indicates whether the volunteer is role playing as a foreign national who is required to provide biometric data upon entering or exiting the U.S. This process will mirror potential airport conditions. Depending on the data required, some test events will assume all volunteers are required to do so.

i. The volunteer proceeds into the sterile departure area (i.e., common departure lounge), which prevents foreign nationals from leaving the sterile area or airport without once again passing through customs and immigration enforcement.

j. The volunteer presents his or her boarding pass to airline representatives in order to board the plane.

k. A DHS representative or contractor addresses issues as needed during the process.

3) **Test Scenario – Mobile Exit Solution:** A fixed biometric collector may be less effective and costly for international airports with very low foreign national traveler throughput or with space limitations. In this case a mobile solution is an option that can be deployed and redeployed between terminals based on passenger flow at larger airports when required.

   a. Using a mobile solution with an integrated barcode reader, the volunteer participant scans his or her boarding pass barcode.

   b. The boarding pass indicates the traveler is a foreign national who is required to provide biometric data prior to departing the country.

   c. The volunteer proceeds to a biometric data collection area prior to the jet bridge.

   d. At the biometric collection area, DHS representatives use a mobile device to capture a high-quality fingerprint, face, or iris image.

   e. The fingerprint, face, or iris image is matched with the biometric and biographic data previously collected.

   f. The volunteer then proceeds to board the plane.

4) **Test Scenario – Jet Bridge Solution:** As volunteers proceed down the jet bridge to board their flight they are instructed to stop and look up at a facial recognition camera that captures facial images of all volunteers (including volunteers posing as U.S. and non-U.S. citizens).

   a. Volunteers proceed to the boarding gate and begin walking down the jet bridge.

   b. All volunteers are asked to stop and look up at a facial recognition camera.

   c. Facial images are matched to data provided by volunteers during the enrollment process.

   d. Volunteers then proceed to board the plane.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[12] articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002[13] states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts privacy impact assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002[14] and the Homeland Security Act. This PIA is conducted as it relates to the DHS construct of the Fair Information Principles because AEER is a project rather than a particular information technology system. This PIA examines the privacy impact of AEER operations as it relates to the Fair Information Principles.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

DHS S&T is contracting with a non-government, third-party to select volunteer participants, collect information from the volunteers, and protect that information. The contractor conducts interviews and informs the volunteers of the test and evaluation activities. The contractor does not share PII with DHS; DHS only receives aggregated data from the contractor such as the False Match Rate (FMR), False Non-Match Rate (FNMR), Failure to Acquire Rate (FTAR), False Rejection Rate (FRR), transaction time, and throughput analysis. The contractor also provides aggregated data about gender, age, nation of origin, and whether English is the volunteer's primary language.

[12] 5 U.S.C. § 552a (http://www.justice.gov/opcl/privstat.htm).
[13] 6 U.S.C. § 142(2) (http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf).
[14] 44 U.S.C. § 3501 note (http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347.htm).

Privacy Risk:

There is a risk that volunteer participants may not understand the information being collected and the uses of that information.

Mitigation:

DHS manages this risk by providing detailed information to the volunteers about what data is being collected and how the contractor and DHS S&T will use it. Volunteers sign informed consent agreements acknowledging they have read relevant explanatory materials and understand what data is being collected and how that data is being used. DHS S&T is limiting the use of PII to test biometric technologies and proposed biometric exit practices and procedures.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Participation is completely voluntary. Volunteer participants sign informed consent agreements that describe the data being collected and the intended uses. Volunteers may withdraw from the study at any time. DHS may ask volunteers to consent to their images being used in subsequent reports and DHS respects the wishes of individuals who prefer not to have their images used in reports by not including them. Participation or lack of participation does not affect a volunteer's ability to travel.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

The test and evaluation activities for AEER are being conducted based on the authority established in the Homeland Security Act,[15] which authorizes DHS S&T to conduct "basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs." In exercising its responsibility under the Homeland Security Act, S&T is authorized to collect information, as appropriate, to support research and development related to improving the security of the homeland. The federal statutes mentioned in the overview of this PIA also require DHS to develop and implement a full biometric entry and exit system.

[15] P.L. No. 107-296, § 302(4) (http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf).

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

The contractor recruiting volunteers for the testing is responsible for collecting, maintaining, and securing the PII of the volunteers as required for follow-up contact, and as required by the IRB. The contractor provides volunteers with an anonymized user identification number for each test. The contractor maintains data for as long as the test is active and for an additional two years in case it is necessary to contact the volunteer.[16] Biometric images are provided to DHS only if a participant has signed an informed consent agreement allowing the contractor to provide biometric data to DHS. There may be instances in which examples (i.e., images) of biometric collection may need to be used to provide clarity in the reports and briefings provided to DHS. Additionally, demonstrations may be conducted from time to time for DHS personnel to observe collection of biometrics during testing scenarios. DHS personnel will only observe the collection of biometric data from participants who have granted permission through informed consent agreements.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

The PII collected by the contractor for this project will remain with the contractor. With the consent of the volunteer, some images of biometric data such as unique fingerprint or iris image patterns will be provided to DHS. DHS S&T will not link the biometric data back to the volunteer. The contractor may only use the data in relation to the test and evaluation project.

Privacy Risk:

There is a risk the information may be used in an unauthorized manner.

Mitigation:

Information collected from volunteers will only be used in accordance with the scope of the test and evaluation project. The scope is clearly stated in the informed consent agreement. AEER is not connected to any outside system, and therefore reduces the risk that information would be shared with any agency or individuals. There is a clear audit trail to ensure that data is

[16] A principal investigator (PI) is a medical doctor acting as the lead scientist and researcher for this effort. If the principal investigator identifies a medical issue during or after the testing, he or she is obligated to notify the volunteer.

being used correctly and administrative actions may take place if information is misused. DHS employees and contractors receive annual privacy training on how to handle PII and steps to ensure that the information will only be used for the purpose for which collected. This risk is also mitigated by limiting access to PII to a small group of contractors with a need to know the information.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

Biometric information is collected directly from the volunteer participants. Researchers notify volunteers that they may view and correct the information, including prior to starting the project, during an initial briefing. Volunteers may correct inaccurate or erroneous information at any time during the project. Since this project is for Research Development Testing and Evaluation (RDT&E) purposes, inaccurate information will have no adverse impact on the volunteer.

As a test and evaluation project, errors that arise during biometric identity verification processes help the researchers determine which products and procedures are most or least accurate. Volunteers will not be adversely affected in the event of errors or inaccuracies arising out of the biometric identity verification processes.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

The contractor protects data by following guidelines established in DHS 4300A Sensitive Systems Handbook. Access to PII is limited to a small group of contractors with a need to know. All biometric images and other data collected from subjects are stored on encrypted media that is kept under lock and key when not in use. The data is stored using anonymous identifiers.

Data linking the anonymous ID to the subject name, address, phone, and other contact/biographical information is stored on encrypted media that is separate from that used for biometric images and other data collected from subjects. Access to this data is restricted to staff assigned responsibility for scheduling appointments or carrying out other administrative tasks by the program manager. Staff with access to this data do not have responsibility for handling/analyzing other data (with the exception of the Principal Investigator). The contractor may directly contact any subject for clarification.

Under some circumstances the IRB or DHS may require access to the contact information for administrative purposes; this is permitted upon written request to the contractor from the

chair of the IRB or the appropriate authority at DHS. Access to this information would be limited to the Office of General Counsel (OGC), the Inspector General (IG), or other auditors.

Researchers participating in the study have access to the biometrics and other information by the anonymous ID only. Researchers are required to sign a data transfer agreement in which they agree not to re-disclose the biometrics and data. Furthermore, the researchers are not permitted to re-identify data provided.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

The contractor conducts regular audits and employs technical safeguards on computer systems on which the volunteers' information is kept. These audits are intended to prevent the misuse of data. The system is isolated and does not accommodate connections from outside machines. The servers are firewall protected and logs are maintained. S&T works with the contractors to ensure those responsible for securing the data have adequate controls in place.

These measures may include:

1. An internal firewall protecting the network to which the workstations are connected.
2. A secondary firewall protecting all servers including email servers and departmental servers.
3. Multi-tiered anti-virus, anti-malware, and anti-spam software and program packages to protect the network.
4. The testing team may audit the network and provide alerts if questionable activity is identified. The team may also initiate a manual process to monitor and investigate any suspicious activity.
5. Network security procedures and practices may be audited by an external agency.
6. The database server is isolated from other networks and is only accessible from the testing devices or from administrator panels on the same network.
7. Planned configuration has client software connecting to the database server using National Institute of Standards and Technology (NIST) information security guidelines.

8. The server is virtualized[17] to add an extra layer of protection for both the server and the system hosting it. Clustering[18] may be added for redundancy and load balancing depending on the needs of the environment.
9. Additional auditing mechanisms that are used during the RDT&E activities depend on the researchers executing the tests; there may be variations of the identified safeguards and audit capabilities in place.

Conclusion

The AEER program tests, evaluates, and develops options to implement congressionally mandated biometric entry and exit requirements. These requirements will improve screening and verifying the identities of foreign nationals arriving at or departing from the United States via U.S. airports. This PIA documents the privacy risks and mitigations associated with this initial testing and evaluation phase. Future phases of this project will require updated or new privacy impact assessments to reassess the privacy risks that emerge in field trials and an operational environment.

Responsible Officials

Robert Burns
APEX Program Manager
Science and Technology Directorate
(202) 254-6104

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

[17] Virtualization limits the potential for computer viruses, Trojan horses, and malware to infect computers and servers.
[18] Clustering allows for a group of servers and other resources to act like a single system enabling high availability, load balancing, and parallel processing.