Privacy Impact Assessment
for the

Iris and Face Technology Demonstration and Evaluation (IFTDE)

August 12, 2010

Contact Point
Arun Vemury
Human Factors/Behavioral Sciences Division
DHS Science & Technology Directorate
(202) 254-6830

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

As part of its Multi-Modal Biometrics Projects, the Department of Homeland Security (DHS) Science & Technology (S&T) Directorate and the National Institute of Standards and Technology (NIST) are investigating iris recognition as a promising biometric modality that may become suitable to support DHS operations in the near future. As iris recognition technologies mature, it is important to understand the capabilities and limitations of the technologies in operational settings, as well as what additional technology development is necessary to reduce technical risk in potential future acquisitions by DHS operational components. The purpose of this evaluation of iris recognition technologies is to conduct field trials/studies of iris camera prototypes under conditions and environments of relevance (e.g., humidity levels, amount of sunlight, etc) to DHS operational users to assess the viability of the technology and its potential operational effectiveness in support of DHS operations. S&T is conducting a PIA because biometric information is being collected from individuals detained in an operational setting.

Overview

This project is managed by the DHS Science and Technology (S&T) Directorate, co-sponsored by the National Programs and Protection Directorate, US-VISIT Program and leverages the joint expertise of DHS, National Institute of Standards and Technology (NIST), Department of Defense (DoD) and the U.S. Naval Academy. Iris recognition is a promising biometric modality that may become suitable to support DHS operations in the future. However, iris recognition has not been systematically and extensively evaluated outside of carefully controlled environments (i.e., in laboratories). The purpose of this evaluation of iris recognition technologies is to conduct field trials/studies of iris camera prototypes under conditions and environments of relevance (e.g., humidity levels, amount of sunlight, etc) to DHS operational users to assess the viability of the technology and its potential operational effectiveness in support of DHS operations.

The iris is a muscle that forms the colored portion of the eye. It regulates the size of the pupil, controlling the amount of light that enters the eye. Although the coloration and structure of the iris is genetically linked, the details of the iris structure are not. Iris imaging requires use of a high quality digital camera that illuminates the iris using near-infrared light and takes a photograph without causing harm or discomfort to the individual. The prototype cameras in this evaluation are designed to capture iris images for different operational scenarios (e.g., standing in front of a mounted or handheld camera or walking near a camera while walking through a portal).

S&T and US-VISIT are working with the DHS Customs and Border Protection (CBP)/ Office of Border Patrol to develop a concept of operations (ConOps) to describe how the technology may be tested to support its existing operational missions. Under an Inter-Agency Agreement (IAA) with DHS, DoD will assist in identifying, integrating, and instrumenting candidate prototype iris cameras for the purpose of in-field evaluation. NIST will conduct the evaluation and analysis in collaboration with Naval Academy researchers on the test data collected during this project to determine the utility of these prototypes. This PIA covers the

collection and use of iris images, facial images, and limited biographic information for purpose of testing and evaluating iris camera prototypes. Iris images will not be used to support any operational decisions. Routine data collection and operational decisions and actions by U.S. Border Patrol are covered under the Enforcement Integrated Database PIA, which can be found on the DHS Privacy Office's public website at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_eid.pdf.

Once identified by the DHS team, the iris camera prototypes will be provided to the U.S. Border Patrol agents. The iris camera prototype includes sensors such as floor-mounted pressure sensors, beam break sensors, motion sensors, and simple cameras. This system works by electronically capturing the iris images of individuals that are placed in front of the camera. The U.S. Border Patrol agents' role in this project is to facilitate the collection of research-related data and iris images, for the purpose of evaluating the functionality of the iris cameras in an operational setting by researchers. The U.S. Border Patrol agents will provide feedback and input on the ease of use and functionality of the prototype to the researchers as well. U.S. Border Patrol agents are one of the envisioned end users of the technology, so it is important to understand and evaluate the usability of the prototype. For example, if it takes U.S. Border Patrol field officers ten minutes to capture one iris image, DHS may re-evaluate the use of that specific prototype system.

To accomplish a thorough and complete analysis and evaluation of the iris camera prototypes, for this research/test researchers require supporting information in addition to the iris images. Supporting information includes limited biographic information (i.e., age, gender, ethnicity, etc.) collected by the U.S. Border Patrol field officers. Partial or full facial images are used for the purpose of quality control (i.e., no iris was collected because the person blinked or the eye was otherwise obfuscated and to ensure the camera does not mislabel a right iris as a left iris). The limited biographic information together with the facial images will assist NIST researchers in determining the accuracy of the iris imaging technology. For example, if it is determined that the technology works with some individuals, but does not work well with people within a specific age range or ethnicity; the technology may be deemed unsuitable for DHS until performance is improved.

During their day to day operations, the U.S. Border Patrol agents collect information from immigrants apprehended for illegally entering the United States. Typically, U.S. Border Patrol agents collect information from these individuals, including a range of personally identifiable information, biographic data, and biometric information (fingerprints, photographs). This information is stored in the US-VISIT (Automated Biometric Identification System (IDENT) database, as described in the joint ICE Enforcement Integrated Database PIA.

For this project, U.S. Border Patrol agents stationed at McAllen, Texas will facilitate the collection of test data over an eight week time period. The agents will continue to conduct their day to day operations and collect and store standard information from individuals apprehended while attempting to enter into the U.S. illegally into the IDENT database. However, in addition to this information, U.S. Border Patrol agents will also collect iris images, using the three different prototype iris cameras provided by DHS/DoD.

The iris camera prototypes are similar to both commercial photographic and video cameras and may incidentally capture partial facial images of the individual along with the iris images. The iris and partial facial images collected by the prototypes during the field evaluation are stored on a protected, stand-alone system. U.S. Border Patrol agents will not process, use or have access to the iris images and partial facial images once they have been saved to the stand alone system. The stand alone system does not have network or Internet connectivity. Additionally, it is not connected to any DHS system (i.e., US-VISIT LAN, IDENT, etc.). No identifying information will be linked or stored with the iris images and partial facial images. The work station information (i.e., work station #1, work station #2) and date and time information are included with the iris images. Some iris image capture cameras may have memory capabilities, however, the equipment is configured to avoid "on board" storage and security protocols clear camera memory at a high rate of frequency. Notice is posted at U.S. Border Patrol stations to provide advance notification of the data collection and inform individuals of the opportunity to opt out of providing iris images.

At the end of the iris image collection period, the iris and partial facial image data are physically transported via FOUO (For Official Use Only) labeled encrypted storage media (i.e., encrypted DVD or encrypted hard drives) to NIST facilities for analysis by NIST. U.S. Naval Academy researchers will go to the NIST campus to access the data and collaborate with the data analysis. No data will be removed from the NIST campus. NIST will then coordinate with US-VISIT to obtain the full facial images and limited biographic data to the corresponding iris images (previously collected by the U.S Border Patrol agents). Using the work station information and date/time stamp, US-VISIT will retrieve from IDENT the corresponding facial image and biographic information (i.e., gender, age, ethnicity) and send it to NIST via email; US-VISIT will properly secure electronic transmission of this information using encryption techniques. US-VISIT will provide this information per an existing process with NIST to support biometric research.[1] US-VISIT will not provide any other identifying information, such as name (of the apprehended individuals or the U.S. Border Patrol agent), to the researchers given that the identity of the individual is not necessary for the project.

All data collected for the project is used for the purposes of biometric image quality and comparison testing and analysis; system interoperability testing and analysis (to determine if iris images produced with one camera can be matched with iris images produced by other cameras); throughput; and performance analysis. All analyses will be conducted by individual researchers using iris quality and matching algorithms; no algorithms will be used to match facial images to each other. The images are not used for any other purposes (i.e., no medical analyses will be conducted using these images, nor will there be any operational decisions based upon analysis of the iris images).

NIST researchers will store the data in an access controlled computer laboratory on the NIST Gaithersburg campus. Physical access is provided using government Personal Identification Cards (PIV) with NIST Police providing continuous door alarm monitoring and is limited to system administrators, project leaders and NIST Police. Network access is only allowed by secure

[1] Decision Record Memo: *Disposition of US-VISIT data with NIST re: 10-Print, Slap Segmentation 2007, and Multi-Modal Support,* 5/25/2007.

networks and is controlled by a firewalled server that limits access to only approved users from approved systems. Naval Academy researchers will review the data at NIST facilities. NIST will not redistribute the biometric and biographic data and will destroy the data at the conclusion of analysis and the end of the project.

S&T will not have access to any information, including iris images, collected during the course of the project. At the conclusion of the project, S&T will receive a final report evaluating each prototype and its utility in an operational environment. The final report may help support future acquisition and deployment decisions.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The Homeland Security Act of 2002 [Public Law 1007-296, §302(4)] authorizes the Science and Technology Directorate 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 R&D related to improving the security of the homeland. The project is an evaluation of prototype iris camera performance under operational conditions and is not considered human subject testing.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The information collection activities described in this PIA are covered by the DHS/S&T 001 Research, Development, Test, and Evaluation Records System of Records Notice. The DHS/S&T 001 Research Records will cover the research, development testing and evaluation of the information.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

This project is a research, development, testing, and evaluation effort; it does not create or set up any IT systems. Therefore a C&A is not required for this project.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. The S&T Records Retention Officer has approved the use of General Retention Schedule (GRS) 20, Item 1a for the retention of the data used to support this research, development, testing, and evaluation effort.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information collected through the law enforcement activities described in this documentation is exempted from collection request requirements of the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

During the course of routine operations, U.S. Border Patrol agents collect personally identifiable information from immigrants that are arrested while illegally crossing the United States-Mexico border. This includes biometric information (full facial images) and biographic information, including gender, age, and ethnicity. U.S. Border Patrol agents maintain this information on the US-VISIT IDENT database. As a participating component in this project, U.S. Border Patrol agents will also collect iris images of detained individuals to test and evaluate the iris image prototype cameras. In addition to the iris images, the prototypes may also capture partial facial images of the individuals.

For this project, U.S. Border Patrol agents will collect and provide the iris images captured by the iris camera prototypes to NIST. The iris image enrollment workstation will require a password to login after a 1-2 minute period of inactivity. Only trained agents with authorized use of the equipment will be given passwords. Naval Academy researchers will go to the NIST campus and collaborate with NIST researchers to conduct analysis at the secured location. Using the work station information and date/time stamp on the iris images, US-VISIT will retrieve from IDENT the corresponding facial image and biographic information (i.e., gender, age, ethnicity) and send it to NIST via email.

The NIST and Naval Academy researchers will use the limited biographic information and facial images to determine potential covariates that may limit the effectiveness of the iris imaging technology in working accurately, or at all. For example, if it is determined that the technology works with some individuals, but does not work well with people within a specific age range or ethnicity, the technology may be deemed unsuitable until performance is improved. Additionally, any full or partial face images produced by the iris cameras are used for the limited purpose of quality control (i.e., no iris was collected because the person blinked or the eye was otherwise obfuscated and to ensure the camera does not mislabel a right iris as a left iris). The full or partial facial images are not used for facial recogntion and are not stored in a format or template suitable for face recognition.

S&T will not receive any information, including iris images, during the course of the tests. S&T will receive a final report at the conclusion of the tests evaluating the utility of the prototypes.

2.2 What are the sources of the information and how is the information collected for the project?

U.S. Border Patrol agents will collect the information and images directly from the individual. Researchers will receive the iris images from U.S. Border Patrol agents. US-VISIT will use the work station information and date/time stamp on the iris image to retrieve the information from the IDENT database and send NIST the limited biographic and full facial images, per existing process.[2]

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

This project does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

The purpose of this research is to evaluate the utility of the prototype iris cameras. Biographic information asserted by the individual is used for limited research purposes and is assumed to be correct, as compared with available identity documentation obtained from the individual. For the purpose of this research, the information is not checked for accuracy. Once the data is stored and saved to the stand-alone system, the U.S. Border Patrol agent will not have access to or manipulate the information. Iris image analysis is performed by examining iris camera instrumentation data and full or partial facial images.

The images and biographic information are only used for research and analysis purposes. Inaccurate information does not affect the individuals or their immigration status.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: A privacy risk associated with data collection is that the data may be used for purposes outside the originally stated purposes (i.e., for testing and evaluation purposes).

Mitigation: To mitigate this risk, the images and biographic data is stored on a standalone system, not connected to any other DHS system or network. The purpose of this project is to test and evaluate the functionality and usability of iris image capture prototypes. Iris image data is separated from other personally identifiable information that is collected by U.S. Border Patrol agents. These steps mitigate privacy risks and help maintain a high level of individual privacy rights. Additionally, the iris images and corresponding biographic information are only used for research, development, testing, and evaluation purposes.

[2] *Ibid.*

Privacy Risk: With the collection of biometric information, a privacy risk may be that inaccurate information may negatively impact the individual.

Mitigation: To mitigate this risk, no identifying information is linked to the iris images or the biographic information used for this project. Researchers will only use the information for research, development, testing, and evaluation purposes; inaccurate information does not impact the individuals or their immigration status. The identity of the individual is not necessary for the research project, and it is not within the scope of the research to identify a specific individual.

Privacy Risk: Finally, a privacy risk may be the unauthorized access or use of the iris images.

Mitigation: To mitigate this risk, user access to the iris image data is limited to authorized NIST and U.S. Naval Academy employees and contractors who are members of the research team. All persons involved with the handling and analysis of biometric data are required to sign the "Rules of Behavior" agreement, which sets forth data handling and access policies for personally identifiable information for this evaluation. To limit access, even S&T employees are not authorized to access the images. All federal government employees and contractors are trained on the use of information in accordance with federal privacy and information security policies, procedures, regulations, and guidance.

DHS Management Directive System (MD) Number: 11042, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, May 11, 2004, provides guidance for the manner in which DHS employees and contractors must handle Sensitive but Unclassified/For Official Use Only Information in both paper and electronic records.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The purpose of this project is to evaluate multiple prototype iris cameras and determine if iris image capture and recognition technologies are capable of functioning in an operational setting in support of DHS operations. If the iris images are of poor quality, iris recognition may not successfully match iris images collected from the same individual using one or more prototype cameras; thus limiting the utility of the technology. The U.S. Border Patrol agents will facilitate data collection for this project; they will not use the iris images or partial facial images captured by the prototypes for any other purposes. Researchers will only use the information for research, development, testing, and evaluation purposes.

Any full or partial facial images produced by the instrumentated iris cameras will be used for the limited purpose of quality control (i.e., iris images were not collected because the person blinked or the eye was otherwise obfuscated and to ensure the camera does not mislabel a right iris as a left iris). The full or partial face images are not used for face recogntion, and are not stored in a format or template suitable for face recognition. Limited biographic data (age, gender, ethnicity, etc.) already collected by U.S. Border Patrol agents during the course of routine

operations is used to identify potential covariates that may limit the effectiveness of the technology in working accurately. For example, if it is determined that the technology works with some individuals but does not work well with people within a specific age range or ethnicity, the technology may be deemed unsuitable until performance is improved.

All persons involved with the handling and analysis of biometric data are required to sign the "Rules of Behavior" agreement, which sets forth data handling and access policies for personally identifiable information for this evaluation. All government and contractor staff are further responsible for complying with applicable privacy and security laws, regulations and policies. Researchers only receive iris or facial images and limited biographic information. Researchers do not receive any identifying information, such as name or address.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

This field evaluation is used for research purposes only. This project does not include electronic searches, queries, or analyses for operational purposes such as predictive pattern or anomaly determinations.

3.3 Are there other components with assigned roles and responsibilities within the system?

DHS S&T provides approximately three prototype iris cameras, ancillary materials (including notice signs), and support for installation and training activities with CBP representatives at a U.S. Border Patrol Station in McAllen, Texas. S&T provides training to U.S. Border Patrol agents and CBP Office of Information Technology (OIT) employees to ensure that the equipment is used properly and ensure notice is visible. In addition to their existing duties to collect information, such as the biographic and biometric information, for apprehension purposes (as described in the joint ICE Enforcement Integrated Database PIA), U.S. Border Patrol agents are responsible for collecting iris images using one or more prototype iris cameras from compliant individuals apprehended for attempting to illegally enter the United States. U.S. Border Patrol agents are not obligated to alter normal processing duties in order to facilitate any additional technical performance measures. U.S. Border Patrol agents are obligated to comply with requests by any individuals who opt out of iris collection research activities, but will continue to collect data required to perform routine operations. U.S. Border Patrol agents and employees are also responsible for limiting unauthorized physical and login access to the iris image collection devices and equipment during the data collection activities at the U.S. Border Patrol Station in McAllen, Texas until the data is removed for secure transfer to NIST.

US-VISIT is providing some funding and supporting program management for the project. US VISIT will also be providing limited demographic information, such as age or ethnicity and facial images of the corresponding iris image, which will be used by NIST in this research project. US-VISIT will not provide any other identifying information, such as name (of

the apprehended individuals or the U.S. Border Patrol agent), to the researchers as the identity of the individual is not necessary for the project.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: Privacy risk associated with the use of the information is that information may be improperly handled.

Mitigation: To mitigate the risk, all persons involved with the handling and analysis of biometric data are required to sign the "Rules of Behavior" agreement, that sets forth data handling and access policies for personally identifiable information for this evaluation. All government and contractor staff are further responsible for complying with applicable privacy and security laws, regulations and policies.

Privacy Risk: Another privacy risk is that information received by the researchers at NIST may be redistributed to researchers or organizations outside the immediate research team.

Mitigation: To prevent redistribution of data from NIST, researchers for the U.S. Naval Academy will go to NIST facilities to view the data. U.S. Naval Academy researchers are required to sign the "Rules of Behavior" agreement, that sets forth data handling and access policies for personally identifiable information for this evaluation. U.S. Naval Academy researchers will not be permitted to remove biometric or biographic data from NIST. NIST will not redistribute the data and will destroy the original biometric and biographic data at the conclusion of their analysis, at the end of the project.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Individuals apprehended by U.S. Border Patrol agents are given notice in the form of English and Spanish signage and oral instruction that (1) information provided to DHS may be used for research purposes, and (2) individuals have the option to opt out of iris image collection processes without consequences to the individual. Signage is posted in locations visible to individuals upon entering the U.S. Border Patrol Station in McAllen, Texas, and prior to entering the collection volume (approximately one cubic meter (1 m^3) or smaller) of each iris camera.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals may consent or decline to provide iris images.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: An associated privacy risk is that individuals are not provided with

sufficient notice of data collection.

Mitigation: To mitigate the risk, notice is provided to immigrants illegally crossing the United States-Mexico border and apprehended by U.S. Border Patrol agents through signs posted at U.S. Border Patrol Stations, and verbal communications. This PIA also serves as notice to the public.

Privacy Risk: Another associated privacy risk is that the data collected for this project will be used for other purposes.

Mitigation: To mitigate this risk, notice is provided to individuals informing them that the use of iris image data is for research and analysis purposes only. The biometric and biographic data will be destroyed by NIST upon completion of the overall project.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

NIST will maintain the information for the duration of the testing and evaluation activities. NIST will maintain this information for the purposes of biometric image quality and comparison testing and analysis; system interoperability testing and analysis (to determine if iris images produced with one camera can be matched with iris images produced by other cameras); throughput and performance analysis. NIST will destroy all the data at the conclusion of the project.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Extended data retention may lead to future unintended or unplanned uses.

Mitigation: A limited amount of biometric and biographic data is collected and used over the life of the project. Once the collection, research, and analyses are completed, researchers will destroy the biometric and biographic data.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

At the end of the eight-week data collection period, U.S. Border Patrol agents will transfer the iris images and partial facial images to NIST researchers that are directly involved and authorized in the research efforts. Researchers from the U.S. Naval Academy will travel to NIST to support research and analysis activities but are not permitted to remove data from NIST.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The purpose of this project is to evaluate the performance and utility of prototype iris cameras in a "real-world" setting. The DHS/S&T 001 SORN, routine use F enables DHS to share the data with "contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records."

6.3 Does the project place limitations on re-dissemination?

NIST and the Naval Academy are not permitted to re-disseminate the data DHS provides. Upon completion of NIST and U.S. Naval Academy research and analyses, NIST will destroy all the biometric and biographic data collected for this project.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

The U.S. Border Patrol maintains a "chain of custody" log. After completion of the iris image collection phase, the U.S. Border Patrol transfers physical custody of the data to NIST. The chain of custody log documents the process and flow of data. US-VISIT and NIST have an existing process, which enables US-VISIT to provide data to NIST to support research.[3]

Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: A privacy risk associated with information sharing is that NIST and U.S. Naval Academy researchers will further disseminate the information or use the information for unauthorized purposes.

Mitigation: To mitigate this risk, NIST and the Naval Academy researchers will sign "Rules of Behavior" documents prior to accessing the information at NIST. NIST and the Naval Academy will use the data for the purposes specified and may not remove any information from the secure NIST facilities. Upon completion of the project, NIST is required to destroy the data provided by DHS.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Due to the nature of this project, individuals do not have access to the iris image data collected by the U.S. Border Patrol or used by NIST or Naval Academy researchers because the iris image data is not linked to a specific individual; personal identifiers are not linked to the iris images, biographic information, or facial images. At the conclusion of the project, all biometric and biographic data will be destroyed, rendering access impossible.

[3] *Ibid.*

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The objectives of this project include testing the capabilities of prototype iris cameras, and analyzing the utility of this equipment in supporting DHS operations. The iris images and limited biographic data are only used for research, test, evaluation and analysis and cannot be deemed inaccurate or erroneous. Inaccurate information does not affect the individual's immigration status and biometric and biographic data will be destroyed at the conclusion of the project. Hence, procedures to correct inaccurate or erroneous information are unnecessary. Once data is collected it will not be accessed or manipulated by U.S. Border Patrol agents.

7.3 How does the project notify individuals about the procedures for correcting their information?

As stated in Section 7.2, the data is collected for research, test, evaluation and analysis and not for operational use. The data cannot be deemed inaccurate or erroneous. Inaccurate information does not affect the individual's immigration status and original biometric and biographic data will be destroyed at the conclusion of the project. Therefore, procedures to notify individuals about how to correct their information are unnecessary.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Lack of redress policies and procedures for those who participate in the project.

Mitigation: Iris images are collected from immigrants arrested for unlawfully entering the United States. The iris images are stored separately from the individual's name. Upon completion of the project, the iris image data will be destroyed. The iris images will not used in any routine DHS immigration and border security operations. The destruction of the anonymized iris image data at the end of this project makes the data impossible to use in other DHS operations, and makes redress policies and procedures unnecessary.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

All persons involved with the handling and analysis of the research data are required to sign the "Rules of Behavior" agreement, which sets forth data handling and access policies for personally identifiable information for this evaluation. All government and contractor staff is further responsible for complying with applicable privacy and security laws, regulations and policies. Researchers only receive iris images, facial images, and limited biographic information. Researchers do not receive information linking the images or information to individual identities. The U.S. Border Patrol agents will have individual access to the iris imaging software, however they will not have access to the stand alone system containing the images. U.S. Border Patrol agents will not have access to any of the iris image data after the images have been collected.

All DHS employees and contractors receive annual privacy awareness training. Additional training for U.S. Border Patrol agents using the prototype iris cameras is provided. The training also includes privacy, security, and acceptable use guidance. DHS provides training to U.S. Border Patrol agents and CBP Office of Information Technology employees and contractors to ensure that the equipment is used properly and that notice is visible.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Only authorized personnel designated by the program manager may access the data. Users may not modify data, but are permitted to organize data as needed to facilitate research and analysis activities.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All new MOUs, information sharing agreements are reviewed by the S&T program manager and legal counsel and then sent to DHS for formal review. Collected data will only be used for research and analysis purposes and will not be used for other purposes. No new access will be granted to organizations within DHS and outside beyond those organizations explicitly cited in this PIA.

Responsible Officials

Arun Vemury

Science & Technology

Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security