Privacy Impact Assessment Update
for the

Customer Profile Management System

DHS/USCIS/PIA-060(a)

July 17, 2017

Contact Point
Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
(202) 272-8030

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The U.S. Citizenship and Immigration Services (USCIS) developed the Customer Profile Management System (CPMS) as a person-centric repository of biometric and biographic information to support USCIS's mission to administer immigration benefits. USCIS currently shares information with various international information sharing partners in accordance with information sharing agreements that are in place between the Department of Homeland Security (DHS) and the foreign governments. USCIS is conducting this Privacy Impact Assessment (PIA) update to discuss the USCIS transition from a manual to automated process to support DHS international data sharing efforts when a match to a USCIS record results in a request for additional information not found in the Automated Biometric Identification System (IDENT) system. At this time, USCIS is only receiving and responding to secondary queries from Canada and Australia. USCIS will update this PIA as USCIS engages with other foreign partners.

Overview

The Department of Homeland Security (DHS) enters into agreements with foreign partners to support the DHS mission, including the U.S. Citizenship and Immigration Services (USCIS) mission to administer immigration benefits. Currently, USCIS exchanges information with Canada and Australia under the Five Country Conference,[1] agreements listed in Appendix A.

The DHS National Protection and Programs Directorate's (NPPD) Office of Biometric Identity Management (OBIM), through the IDENT,[2] supports the initial query and response process for international biometric sharing.[3] IDENT serves as the central DHS-wide system for the storage and processing of biometric data. IDENT stores and processes biometric data—digital fingerprints, photographs, iris scans, and facial images—and links biometrics with biographic information to establish and to verify identities.

Authorized IDENT users query IDENT and may also use IDENT to store their biometric and associated biographic information. As authorized IDENT users, foreign partners and USCIS are able to search and enroll biometric and associated biographic data in IDENT. IDENT may, upon USCIS approval, share USCIS biometrics and limited biographic information with other DHS Components, federal, state, local, or foreign governmental agencies, when DHS determines that the receiving agency has a need-to-know to carry out national security, law enforcement,

[1] The Five Country Conference (FCC) is a forum for cooperation on migration and border security between the countries of Australia, Canada, New Zealand, the United Kingdom, and the United States (collectively called the FCC partners).
[2] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy. The IDENT PIA and appendices discuss that process in more detail.
[3] IDENT is the central DHS-wide system for the storage and processing of biometric and associated biographic information for national security, law enforcement, immigration and border management, and intelligence purposes, and is also used to conduct background investigations for national security positions and certain positions of public trust.

immigration, intelligence, or other DHS-mission-related functions, consistent with the Privacy Act and departmental policy. Through IDENT, OBIM provides the results of biometric checks to authorized users in order to help them accurately identify individuals they encounter pursuant to their missions, including determinations of whether those individuals pose possible threats to the United States. The IDENT PIA appendices outline all data sharing arrangements currently supported by DHS. The users' responses may include some or all the information from an individual's previous IDENT encounters but does not include all USCIS information contained in the Alien File (A-File).

The DHS approach to international information sharing is a coordinated effort that leverages capabilities across multiple DHS offices and Components. Currently, these information sharing processes are segmented, manually-based, and include multiple network connections between countries and components to share information. To streamline international information sharing and create efficiencies required to obtain information about an individual in a more timely fashion, USCIS developed a technical solution using a combination of the Customer Profile Management System (CPMS)[4] and the International Case Tracking System (ICTS) [5] to query and respond to foreign partners through IDENT. When a query from a foreign partner results in a match in IDENT, IDENT sends a request to CPMS, CPMS then sends the country-specific request to the ICTS. As a carry-over from the existing manual process, each country uses its own information request template, but generally shares the record subject's associated biographic information (such as IDENT Fingerprint Identification Number (FIN), Alien Number (A-Number), and full name), Foreign Partner Identification Number, and requested information and documentation. USCIS is developing a uniform template for use with all foreign partners. CPMS stores all query and response data to and from the foreign partner that results from the requests for additional information.

***USCIS Initiated Query*:**

Currently, to support the adjudication of the asylum and refugee benefit process, the Refugee Asylum International Operations Directorate (RAIO) sends queries through a manual email and spreadsheet process to IDENT on asylum and refugee cases. IDENT sends the queries to Canada and Australia only. With this update, an asylum or refugee officer assigned to a case can now use CPMS to request a query to a foreign partner on an individual. CPMS initiates a fingerprint query of foreign partner data through the IDENT system. When the query results in a match to data in the foreign partner's database, the foreign partner returns a response through IDENT that indicates a match and also returns limited biographic data elements that are stored in IDENT as part of an encounter. The initial response minimizes the amount of data provided to querying partner to only what is necessary to confirm the identity. If there is no match on a

[4] *See* DHS/USCIS/PIA-060 Customer Profile Management System (CPMS), *available at* www.dhs.gov/privacy.
[5] *See* DHS/USCIS/PIA-069 International Case Tracking System, *available at* www.dhs.gov/privacy.

biometric query, the foreign partner returns a "no match" response and the response is stored in CPMS.

When a USCIS-initiated query results in a match in the foreign partner system, IDENT automatically sends a second query that may result in the foreign partner providing additional information. When further data is needed, USCIS may send a third query and receive a third response.

CPMS stores all USCIS queries and the foreign partners' responses to USCIS when additional information is sought. In addition, pertinent information for the adjudication of the benefit may be printed and stored in the A-File.[6] The Fraud Detection National Security (FDNS) analysts assigned to the RAIO may also use the results from the international data sharing efforts to conduct potential fraud investigations.[7]

***Foreign Partner Query*:**

The foreign partner query process is the same as the USCIS query process, in that IDENT is the primary interface and CPMS and ICTS are the USCIS systems used to automate USCIS responses. The foreign partner initiates a fingerprint query in IDENT, then IDENT returns an automated response of "match" or "no match."[8] If there is a match, limited biographic information stored in IDENT (outlined below) is provided. The specific data elements are outlined in the IDENT PIA referenced above. If the foreign partner needs additional information to assist in the adjudication of its benefit, the foreign partner may request DHS, through IDENT, to provide additional information.[9] If USCIS is the original source of the biometrics matched in IDENT, the foreign partner request is routed to CPMS.

CPMS automatically checks to see whether any individuals matched through a query to IDENT has a protected status/class in the Central Index System (CIS) via Person Centric Query System (PCQS).[10] When the CIS indicates there is protected status/class, and it is therefore not permissible to share the information with the foreign partner, USCIS may send a "no match" response to the foreign partner through IDENT.

---

[6] Alien Files, or "A-Files," are individual files identified by subject's Alien Registration Number ("A-number"). An A-number is a unique personal identifier assigned to a non-citizen. A-Files became the official file for all immigration and naturalization records created or consolidated since April 1, 1944.

[7] *See* DHS/USCIS/PIA-013 Fraud Detection and National Security Directorate (FDNS), *available at* www.dhs.gov/privacy to learn more about FDNS's processes and information technology systems.

[8] If the new encounter matches an identity in the system, then IDENT appends the encounter to the existing encounters for that identity. If the identity does not match records stored in IDENT, then it is identified as a no match.

[9] Currently, only Canada and Australia may request additional information from USCIS.

[10] Examples of Special Protected Classes include, T, U, and Violence Against Women Act (VAWA), Asylum and Refugee information (i.e., 8 U.S.C. § 1367 and 8 U.S.C. § 208.6). There are different requirements depending on which special protected class is implicated.

If the individual does not have a protected status, CPMS then sends the foreign partner query to ICTS. USCIS uses ICTS to receive and respond to foreign partner queries via CPMS. USCIS analysts use ICTS to prepare responses to the foreign partner inquiries. Responses, may include the original request and scanned documents requested by the foreign partner. This information is uploaded into ICTS and the package is electronically transmitted to CPMS. OBIM analysts retrieve the documents from CPMS and share the information with the foreign partners. CPMS stores those queries and the response that USCIS sends back to the foreign partner as well.

An additional process may occur when an incoming foreign partner query results in a match. If USCIS determines the information may be useful to support the USCIS mission, USCIS may request specific information on that individual from the foreign partner, to augment the existing USCIS record.

Reason for the PIA Update

USCIS is updating this PIA to discuss USCIS automated support of DHS international biometric-based sharing efforts using CPMS and ICTS.[11] Previously, USCIS supported queries and requests for additional information through a manual email process, which was cumbersome, time consuming, and created data quality risks due to manual data entry errors. To improve efficiency and mitigate the data quality risks, USCIS automated the email process by developing a CPMS to ICTS system-to-system solution. In addition to improving data quality, the system to system solution is more secure than the use of emails, which could inadvertently be sent to an unauthorized person or potentially be intercepted during transmission. Moreover, the use of CPMS and ICTS allows USCIS to easily track, monitor, and report on international information sharing and accurately account for disclosures. The new automated process can handle a greater volume of queries, thus creating efficiencies required to obtain the necessary information about individuals in a timely manner.

CPMS interfaces through IDENT with the biometric systems of foreign partners in which a signed information sharing agreement and appropriate waivers[12] are in place. The process of all query and response interfaces with the foreign partner through IDENT remains constant. The new development is an automated process whereby CPMS will store and send the responses created in ICTS to support the requests for additional information from foreign partners. CPMS also stores the foreign partners' responses to USCIS queries.

[11] *See* DHS/USCIS/PIA-069 International Case Tracking System (ICTS), *available at* www.dhs.gov/privacy.
[12] 8 CFR 208.6 generally prohibits the disclosure to third parties of information contained in or pertaining to asylum applications, credible fear determinations, and reasonable fear determination absent the applicant's signed written consent or the written authorization of the Secretary of Homeland Security.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

The legal authority to collect biometric and associated biographic information, including Social Security numbers (SSN), does not change with this update. A full list of current DHS Agreements with Five Country Conference partners may be found in Appendix A.

The collection, use, maintenance, and dissemination of information are covered under DHS/USCIS-002 Background Check Service (BCS)[13] and DHS/USCIS-003 Biometric Storage Systems (BSS)[14] SORNs. USCIS is currently consolidating these SORNs. Once published, the BCS and BSS SORNs will be retired.

This update does not change the Authority to Operate (ATO) for CPMS. USCIS issued the ATO for CPMS on October 31, 2014, and is part of an Ongoing Authorization program. As such, CPMS will have an ongoing ATO with no expiration date as long as CPMS continues to operate in compliance with security and privacy requirements.

The records schedule does not change with this update. Data will be retained for 100 years from the individual's date of birth in accordance with NARA Disposition Authority Number DAA-0563-2013-0001-0005.

This update does not impact the Paperwork Reduction Act requirements for CPMS activities. Biometrics collections are subject to the PRA and currently they are accounted for under each information collection (i.e., applications and petitions) that requires its collection to account for the burden. Additionally, Identity Verification Tool (IVT) is subject to the requirements set forth by PRA.[15] Form M-1061, *Information About the Customer Identity Verification Program and the Secondary Inspections Tools* (OMB Control Number 1615-0125), which is an informational flyer, covers the biometric collection through IVT.

Characterization of the Information

For the purpose of international data sharing, USCIS may receive data from a foreign partner under the terms of a signed information sharing agreement that defines the authorized data sets. CPMS supports both USCIS-initiated and foreign partner-initiated queries and responses when additional information is sought. CPMS stores foreign partner query data and the response created by the ICTS. In addition, it will store foreign partner responses to USCIS queries.

---

[13] *See* DHS/USCIS-002 Background Check Service, 72 FR 31082 (June 5, 2007).
[14] *See* DHS/USCIS-003 Biometric Storage System, 72 FR 17172 (Apr. 6, 2007).
[15] IVT is an Internet-based tool that retrieves, processes, and displays biometric and biographic data from the Automated Biometric Identification System. IVT displays applicant photos and information allowing visual verification of identity and biometric capturing prior to adjudication.

The requests from the foreign partner may include:

- Requestor name and contact information;
- Date of request;
- Reason for request (e.g., Visa applicant, application, refugee claimant, enforcement, and absconder);
- Prioritization (high, medium, or low);
- Full name;
- Date of birth;
- Country of birth;
- Gender;
- Alias; and
- Encounter Identifier (IDENT Encounter Identifier (EID) or foreign fingerprint identifier).[16]

The response may include but is not limited to:

- Reviewer name and contact information;
- Date of response;
- Name;
- Date of birth;
- Alien Number;
- IDENT Fingerprint Identification Number or foreign partner identifier;
- Gender;
- Race;
- Country of birth;
- Country of Citizenship;
- Immigration status;
- IDENT or foreign partner watchlist status (status date and type);

[16] The IDENT EID is an IDENT generated number. *See* DHS/NPPD/OBIM/PIA-002 IDENT, *available at* www.dhs.gov/privacy.

- Photographs; and
- Document images (passport, visas, marriage licenses, etc.).

USCIS relies on the accuracy of data sent by the foreign partner but also conducts accuracy checks through the ICTS case file review outlined in the ICTS PIA.

Uses of the Information

The CPMS technical solution supports DHS data sharing efforts with foreign partners. USCIS queries foreign partner data to assist in the determination of immigration benefits. Knowledge of that benefit determination supports effective adjudication of USCIS immigration benefits.

Privacy Risk: There is a risk the new information in CPMS will be used for a purpose not compatible with the international agreements.

Mitigation: The data collected in CPMS from the foreign partners will continue to be used to administer immigration benefits and support international data sharing efforts in alignment with the USCIS mission. For instance an individual who has already received asylum in another country may not be entitled to receive asylum in the United States. In addition, the new information in CPMS may be used by USCIS FDNS to assist in identifying identity fraud, when an individual may be trying to gain immigration benefits using a fraudulent identity. The foreign partner data stored in CPMS is sequestered from all other data which further restricts access to only the administration of USCIS immigration benefits.

Notice

USCIS is providing notice about the automated exchange of information with foreign partners through this PIA update. USCIS is also publishing a new SORN to provide additional transparency to the biometric check, and biographic background check, identity verification and resolution, card production record systems, and data sharing efforts. This SORN provides details about the international data sharing support. In addition, USCIS form instructions include Privacy Act Statements that states that benefit request form data may be shared with foreign governments.

Privacy Risk: There is a risk that data shared through the international agreements may not be accurate.

Mitigation: USCIS and the foreign partners mitigate this risk by providing notice of the use and sharing of data through these agreements and by providing record access and correction capabilities. USCIS redress processes do not change with this update. The IDENT PIA provides links to foreign partner redress processes.

Data Retention by the project

Data retention does not change with this update. USCIS will retain foreign partner information in accordance with NARA Disposition Authority Number DAA-0563-2013-0001-0005.

Information Sharing

DHS components have access to foreign partner data stored in IDENT. USCIS is updating the CPMS PIA to discuss how CPMS supports the automated DHS international data sharing initiatives through IDENT when additional information is sought. CPMS interfaces through IDENT with the biometric systems of Five Country Conference partners and other foreign countries when a signed information sharing agreement and appropriate waivers are in place. Currently CPMS submits initial queries through IDENT and IDENT submits and receives queries to and from the foreign partner. The new development is an automated process whereby CPMS will store and send the responses created in the ICTS to support the requests for additional information from foreign partners through IDENT.

Redress

USCIS continues to provide individuals with the ability to file a Freedom of Information Act (FOIA) and/or Privacy Act (PA) request to gain access to or amend their USCIS records as appropriate as outlined in the published CPMS PIA. People not covered by the Privacy Act or Judicial Redress Act (JRA) still may obtain access to records consistent with FOIA unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. Any individual seeking to access to his or her information should direct his or her request to USCIS National Records Center (NRC), P.O. Box 648010, Lee's Summit, MO 64064-8010. If a person finds inaccurate information in his or her record received through FOIA, he or she may visit a local USCIS Field Office to identify and amend inaccurate records with evidence.

Auditing and Accountability

USCIS developed an International Integrated Project Team (IPT) to manage all international data sharing efforts. Participants from impacted Programs and Directorates, the Office of Chief Counsel, and the Office of Privacy participate. The IPT monitors the development and implementation of new agreements and ensures protection of records through the development of system requirements and filtering tools.

The USCIS International IPT supports the Departmental negotiation of all information sharing agreements. While the DHS Office of Policy leads international data sharing policy efforts for DHS, and U.S. Immigration and Customs Enforcement (ICE) Law Enforcement Information Sharing Initiative (LEISI) manages the operational aspect and the implementation of the

agreements, other DHS components including USCIS are included in various parts of the process and tasked with reviewing operational protocols.

Responsible Official

Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Appendix A

Five Country Conference Agreements and Related Documentation:

1. High Value Data Sharing Protocol Memorandum of Understanding between The Australian Department of Immigration and Citizenship (DIAC) and the United States Homeland Security and the United States Department of Homeland Security (DHS) and the United States Department of State (DoS).
2. Letter of Agreement to amend the High Value Data Sharing Protocol Memorandum of Understanding between The Australian Department of Immigration and Citizenship (DIAC) and the United States Homeland Security and the United States Department of Homeland Security (DHS) and the United States Department of State (DoS).
3. Agreement Between the United States of America and The Government of Australia For the Sharing of Visa and Immigration Information - Signed at Canberra August 27, 2014.
4. Implementing arrangement between Department of Immigration and Border Protection of Australia and DHS– Signed at London, September 9, 2015.
5. Disclosure of Asylum-Related Information to the Foreign Government Participants on the Five Country Conference," Secretary Napolitano, March 5, 2010.
6. Implementing Arrangement between the Department of State and the Department of Homeland Security of the United States of America, on the one side, And the Department of Citizenship and Immigration of Canada and the Canada Border Services Agency, on the other side, concerning Biometric Visa and Immigration Information Sharing (May 2015).
7. Annex to the 2003 Statement of Mutual Understanding on Information Sharing regarding the Sharing of Information Under the Five Country Conference High Value Data Sharing Protocol between the Department of Citizenship and Immigration Canada (CIC).
8. Disclosure of Asylum-Related Information to the Foreign Government Participants on the Five Country Conference, 2016.
9. The Agreement between the Government of Canada and the Government of the United States of America for the Sharing of Visa and Immigration Information (December 13, 2012).
10. The Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America for the Sharing of Visa, Immigration, and Nationality Information (April18, 2013).