Privacy Impact Assessment
for the

Customer Profile Management Service (CPMS)

DHS/USCIS/PIA-060

December 17, 2015

Contact Point
Donald Hawkins
USCIS Privacy Officer
United States Citizenship and Immigration Services
(202) 272-8000

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

Abstract

The United States Citizenship and Immigration Services (USCIS) developed the Customer Profile Management Service (CPMS) to replace the Biometric Storage System (BSS), the Image Storage and Retrieval System (ISRS), and aspects of the Benefits Biometrics Support System (BBSS). CPMS supports USCIS's mission to administer immigration benefits by serving as a person-centric repository of biometric and biographic information provided by petitioners and applicants (hereafter collectively referred to as "benefit requestors") that have been issued a USCIS card evidencing the granting of an immigration related benefit (i.e., permanent residency, work authorization, travel documents). USCIS is conducting this Privacy Impact Assessment (PIA) because CPMS collects, stores, and shares personally identifiable information (PII). Upon publication of this PIA, the BSS PIA will be retired.

Overview

The Department of Homeland Security (DHS) U.S. Citizenship and Immigration Services (USCIS) oversees lawful immigration to the United States. USCIS receives and adjudicates benefit request forms for all U.S. immigration and non-immigrant benefits. USCIS captures biographic and biometric data from benefit requestors to facilitate three key operational functions: (1) conduct name and fingerprint-based background checks against external systems; (2) verify benefit requestor's identity; and (3) produce benefit cards/documents. Previously, USCIS stored biometric and biographic data in multiple systems. There are inherent risks associated with the duplication of data, including a greater potential for data inaccuracy occurring when duplicated data in one system is updated or corrected without doing the same in the system of origin.

USCIS recognized this risk and developed CPMS to centralize all biometric and biographic data into a single repository. The purpose of CPMS is to: (1) replace the Image Storage and Retrieval System (ISRS), Biometric Storage System (BSS), and aspects of the Benefits Biometrics Support System (BBSS); (2) serve as the centralized repository of biometrics captured by USCIS; (3) serve as the centralized authoritative source of image sets for benefit card and document production; and (4) facilitate identity verification. CPMS benefits USCIS's mission by consolidating biometric and biographic data in a centralized, person-centric, searchable repository.

USCIS Biometric Storage

CPMS serves as the new repository for all biometric data by USCIS captures from benefit requestors filing in support of designated benefit requests. This new system replaces ISRS and BSS. ISRS and BSS were legacy systems that stored a limited amount of information related to

10-print fingerprints and card production information. CPMS consolidates storage of information from multiple, separate systems into a single database, allowing for greater control, security, and management of the data. CPMS also sends fingerprints, photographs, and limited biographic information to the Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT), but CPMS remains the authoritative repository of USCIS biometrics.[1]

USCIS schedules individuals to be fingerprinted after they file a benefit request form indicating that the benefit request requires biometrics. USCIS uses the National Appointment Scheduling System (NASS) to schedule applicants for biometric collection appointments.[2] NASS connects to CPMS to vet pending benefit requestors through a series of parameters to determine if the capture of biometric data is required. NASS accesses the CPMS Application Support Center (ASC) Encounter Data Query Service to determine whether USCIS has photos or fingerprints of applicants on file. If fingerprints are on file, CPMS ASC Encounter Data Query Service determines whether or not the fingerprints on file are current. If the biometrics are current, USCIS does not need to collect additional biometrics. The queries performed on the benefit requestor include the receipt number, biometric query, background check, and refresh check. CPMS returns a message to NASS indicating which, if any, biometrics need to be scheduled. If needed, NASS then generates and sends a biometric appointment notice to the benefit requestor and his or her attorney or representative.

The biometric collection process begins with the capture of biometric data at an authorized biometric capture site, including USCIS offices, ASCs, or U.S. consular offices and military installations abroad using USCIS LiveScan.[3] USCIS uses LiveScan electronic fingerprint scanning systems to digitally capture and electronically submit applicant fingerprint images. The fingerprints are used to conduct criminal background checks prior to USCIS making a determination whether to grant immigration benefits to applicants. LiveScan submits the collected information to CPMS through the Enterprise Service Bus (ESB).[4]

At the ASC, USCIS electronically captures the benefit requestor's fingerprints (hereafter referred to as "10-prints") and related biographic data required to verify the individual's identity and to ensure that the correct biographic information is associated with the captured biometrics. For some benefits, when a benefit requestor arrives for a scheduled benefit interview at a USCIS Field or Asylum Office, USCIS asks him or her to provide two fingerprints. USCIS uses the two fingerprints to electronically verify the benefit requestor's identity by comparing the two

[1] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy.
[2] *See* DHS/USCIS/PIA-057 National Appointment Scheduling System (NASS), *available at* www.dhs.gov/privacy.
[3] The LiveScan software is run on USCIS computers and is used to capture biometric and biographical information from applicants domestically and internationally. The LiveScan software is also available as a mobile device to capture biometrics at refugee camps.
[4] *See* DHS/USCIS/PIA-008 Enterprise Service Bus (ESB), *available at* www.dhs.gov/privacy.

fingerprints to stored encounters and the captured fingerprints by DHS.

CPMS provides ASC encounter biometric data to USCIS's Electronic Immigration System (ELIS) through Person Centric Query Service (PCQS) using the CPMS ASC Encounter Query Service to support scheduling and card printing.[5] For card production purposes, ELIS sends the retrieved biometrics so that the appropriate card can be produced by the Enterprise Print Management Service (EPMS). All requests, responses, and queries flow through the ESB.

CPMS also sends fingerprints, photograph, and limited biographic information to the Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT).[6] IDENT serves as the DHS-wide IT system for the storage and processing of biometric data. IDENT stores and processes biometric data from across DHS—digital fingerprints, photographs, iris scans, and facial images—and links biometrics with biographic information to establish and verify identities. When a biometric is submitted to IDENT for an individual and it is his or her first enrollment in IDENT, a unique identifier is assigned—the Fingerprint Identification Number (FIN). The unique enumerator is based on and assigned to an individual's unique fingerprint biometric signature. If IDENT does not find a match, the system enrolls the fingerprints, generates a unique enumerator, and returns the FIN to CPMS.

IDENT is organized by fingerprint matches and documents associated to specific fingerprint encounters. Information collected through CPMS includes biometrics and more expansive biographic information related to specific benefits requirements; the additional biographic information exceeds the scope of biometric and biographic encounter information that IDENT maintains. IDENT may share CPMS 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 the information to carry out national security, law enforcement, immigration, intelligence, or other DHS-mission-related functions, consistent with the Privacy Act.

Background and Verification Checks

CPMS facilitates OBIM, Department of Justice Federal Bureau of Investigation (FBI), and Department of Defense (DoD) background and verification checks. CPMS maintains the background check results to assist USCIS with the adjudication of the requested benefit.

IDENT Verification Checks

USCIS developed the CPMS IDENTity Verification Tool (IVT), an internet-based application, to verify an applicant's identity before an interview or appearance at an USCIS

[5] *See* DHS/USCIS/PIA-010 Person Centric Query Service (PCQS) and DHS/USCIS/PIA-056 USCIS ELIS: Form I-90, *available at* www.dhs.gov/privacy.
[6] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy.

office. IVT processes, retrieves, and displays biometric and biographic data from IDENT. IVT provides USCIS with the capability to compare an individual's biometric and biographic information to previous biometric encounters contained within IDENT. IVT replaces the Secondary Inspections Tool, contained within IDENT, which is currently in use at USCIS Field and Asylum offices.[7]

USCIS uses IVT to verify the identity of the individual at the time of an in-person interview or when the individual appears at an USCIS office to obtain documentation evidencing an immigration benefit. Individuals are required to have their photograph and fingerprints taken at a USCIS office to be entered into the IVT. The USCIS Immigration Services Officer (ISO) asks the applicant to place his or her index fingers on the fingerprint scanner, which electronically scans his or her fingerprints and sends them to IDENT for comparison and matching.[8] In addition, the USCIS ISO takes a digital photograph of the benefit requestor, which is stored in the IDENT database.[9]

USCIS also enters biographic data into IVT. ISOs may manually enter one of four identifiers: the Alien Number (A-number), Encounter Identification Number (EID), FIN, or Receipt Number to search for encounter records in the IDENT database. IVT uses biometric and biographic data to retrieve a complete list of DHS encounters associated with the individual's biographic and presented biometric data in IDENT. This complete list of encounters may include an application for a visa to enter the United States, entries and exits from the United States, and whether the benefit requestor is of interest to United States or international law enforcement or intelligence agencies because of suspected or confirmed illegal activity.

USCIS ISOs print the list of encounters, along with the associated information, and place it in the benefit requestor's Alien file (A-File) or temporary file (T-file).[10] Captured fingerprint images are not retained within the A-File or T-File. The ISO uses these files for adjudication purposes during the interview process.

Federal Bureau of Investigation (FBI) Name-Based Background Checks

CPMS replaces the existing FBI name check process.[11] USCIS uses CPMS, through the ESB, to send benefit requestor information (name, date of birth (DOB), country of birth, race, and gender) to the FBI to conduct a name check. The FBI Name Check is a name-based search

[7] The DHS/USCIS/PIA-014 Customer Identity Verification (CIV) System Pilot and update will be retired upon publication of this PIA.
[8] When paired with a scanner to capture index fingerprints, the tool affords 1:1 biometric verification between IDENT's stored encounters and the captured prints. Other fingers may be used in the absence of index fingers.
[9] This is the same set of information that is currently collected by IDENT as part of U. S. Customs and Border Protection's existing process for conducting an identity check upon an alien's entry into the country.
[10] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (Nov. 21, 2013).
[11] *See* DHS/USCIS/PIA-033 Immigration Benefits Background Check Systems (IBBCS), *available at* www.dhs.gov/privacy.

of the FBI's Central Records System (CRS) and Universal Index (UNI).[12] CRS contains FBI investigative, administrative, criminal, personnel, and other files compiled for law enforcement and national security purposes. UNI consists of administrative, benefit requestor, criminal, personnel, and other law enforcement files.

The FBI responds to the FBI Name Check with either a: "no record," "positive response," or "pending." A no record response means that the FBI has no relevant information based on the name and DOB of the benefit requestor. A pending response means further research is needed before the FBI can provide a final response. For those records with an initial response of pending, the FBI will complete a review of its records and provide a final response of no record or positive response. A positive response means the FBI has information relating to the subject, which is obtained by USCIS officers through separate processes outside of CPMS.[13] All FBI Name Check requests, responses, and queries flow through ESB; there is no direct connection between the FBI's biographic Name Check processing and CPMS.

FBI Fingerprint-Based Background Checks

CPMS replaces the FBI fingerprint check capability of the BBSS. USCIS simultaneously sends benefit requestor information to include, name, DOB, country of birth, race, gender, address, and biometric images, (including photographs and fingerprints) to both IDENT and FBI Next Generation Identification (NGI) in order to conduct the fingerprint background check.[14] NGI contains FBI criminal history record information compiled from law enforcement and national security submitters.[15] The FBI fingerprint check is an image-based search of NGI.

The FBI responds to the fingerprint check with either a: "Non-Match," "Match," or unclassifiable. A Non-Match response means that the FBI has no criminal history information related to the fingerprints captured from the benefit requestor. A Match response means the FBI has criminal history information relating to the fingerprints submitted. A Match response is usually accompanied by the Identity History Summary, previously known as the Record of Arrest and Prosecution Sheet (RAP Sheet). An unclassifiable response means the fingerprint image quality was too poor to compare against fingerprint records contained within IDENT and NGI. For those records with an initial response of unclassifiable, USCIS captures and submits

[12] *See* DOJ/FBI-002 Central Records System (CRS), 66 FR 29994 (June 4, 2001).
[13] The FBI sends the actual information in a Letterhead Memorandum relating to the positive response separately via encrypted email or over the classified network. The memoranda are stored in the A-File and if the memoranda are classified, then the A-File becomes classified. Records for refugees are stored in FD-258 MF. FD-258 MF existed prior to CPMS to make the FBI responses (both Biometric and Name check) available to analysts and officers using the Central Index System. *See* DHS/USCIS/PIA-033 Immigration Benefits Background Check Systems (IBBCS) for more information on FD-258MF.
[14] The FBI replaced its Integrated Automated Fingerprint Identification System (IAFIS) with the Next Generation Identification (NGI). Please see the Privacy Impact Assessment
Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Biometric Interoperability for more information, available at https://www.fbi.gov/foia/privacy-impact-assessments/iafis-ngi-interoperability-1.
[15] *See* DOJ/FBI-002 Central Records System (CRS), 66 FR 29994 (June 4, 2001).

additional fingerprints to obtain a valid response. All FBI fingerprint check requests and responses are routed to NGI via the ESB and IDENT. There is no direct connection between the FBI's NGI and CPMS.

DoD Fingerprint-Based Background Checks

USCIS uses the LiveScan to capture biographic and biometric information for applicants seeking immigration benefits from USCIS. CPMS, via ESB, sends the benefit requestor's date of birth, country of birth, race, ethnicity, weight, height, eye color, hair color, gender, address, and biometric images (i.e., fingerprints, photograph, and signature) to DoD in order to conduct the fingerprint background check. The DoD fingerprint check is an image-based search of the DoD's Automated Biometric Identification System (ABIS).[16] ABIS contains DoD encounter history information compiled during its operations and from individuals seeking access to its installations. USCIS only sends fingerprints to ABIS for specific benefit types when the beneficiary has a higher likelihood of having previously been fingerprinted by the U.S. military. Currently, those specific benefit types are refugee, asylum, and international relative petitions related to those benefit types.[17]

DoD responds to the fingerprint check with either a: "Non-Match" or "Match" response. A Non-Match response means that DoD has no encounter history information related to the fingerprints submitted by the benefit requestor. A Match response means DoD had obtained fingerprints from the same individual who had submitted fingerprints to USCIS. Match responses are accompanied by pertinent text explaining the nature of the previous DoD encounter. All DoD fingerprint check requests and responses currently flow through CPMS via ESB. There is no direct connection between ABIS and CPMS.

Card Production Information

USCIS issues cards and documents to individuals who have been granted immigration benefits such as Permanent Resident Cards. CPMS is the centralized source of biometric images used for USCIS benefit card and document production. CPMS stores information regarding benefit card and document production, including photographs, signatures, press-prints (one fingerprint image, typically the index finger), and card production status.

Biometric and biographic data are sent from the respective USCIS case management system to the print production systems, where a card is produced. Applications processed by Computer Linked Application Information Management System (CLAIMS) 3[18] are sent to the Integrated Card Production System (ICPS) and Travel Document Processing System (TDPS) so that the

[16] Department of Defense Detainee Biometric Information System, 72 FR 14534 (Mar. 28, 2007).
[17] DoD retention of these biometrics varies based on benefit type.
[18] *See* DHS/USCIS/PIA-016 - Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3), *available at* www.dhs.gov/privacy.

associated card evidencing a beneficiary's status can be produced. Applications processed by ELIS are sent to Enterprise Print Management Service (EPMS).

CPMS interfaces with these systems via ESB to transmit appropriate data for card production. It also tracks and receives card issuance status. CPMS receives data linked with benefit cards and documents, including: card serial number; receipt number; production site; production date; class of admission; type of benefit card or document; and expiration date. After the card is produced, a record (including biometrics and related biographic data) is sent electronically to CPMS via ESB on a daily basis.

Collection and Use of Information

All information stored in CPMS is collected as part of the USCIS benefit request form administration and adjudication process. USCIS requires biographic, biometric, and background check information to verify the benefit requestor's identity and eligibility for the benefit request. U.S. Immigration and Customs Enforcement (ICE), U.S. Customs and Border Protection (CBP), OBIM, and the Department of State (DoS) have read-only access to the CPMS through a web-based user interface, or through Person-Centric Query Service (PCQS).[19]

CPMS offers internal and external users two modes of access to CPMS data:

1. **CPMS User Interface (UI)**: CPMS provides users with an active directory account permissions to query CPMS and view biographic images (photo, signature, and press-print image) of USCIS benefit recipients through the CPMS user interface. CPMS UI allows users to search for individuals based on name and date of birth combination, A-Number, receipt number, or card serial number. Results are displayed as a list of person matches; users can then click on a match to view details of cards granted to that individual. USCIS, ICE, and CBP have access to CPMS UI for identity verification and fraud detection.
2. **Person-Centric Query Service (PCQS):** CPMS offers a PCQS interface through the ESB that enables PCQS users (who do not have a CPMS user account) to retrieve CPMS data.[20] To perform a person search, the user uses the following information to retrieve CPMS data via PCQS: full name, A-Number, Social Security number (SSN), receipt number, ELIS Account Number, and transaction control number. The results are formatted into a single response message and returned to the requestor. PCQS returns the following information: first name, last name, date of birth, A-Number, and card data, which includes A-Number, country of birth, receipt number, card serial number and card production date, card expiration date, biometric capture date, form name, signature, fingerprint press-

[19] *See* DHS/USCIS/PIA-010 Person Centric Query Service (PCQS), *available at* www.dhs.gov/privacy.
[20] *See* DHS/USCIS/PIA-010 Person Centric Query Service (PCQS), *available at* www.dhs.gov/privacy.

print, and photo. ICE, CBP, OBIM,[21] and DoS have access to CPMS data via PCQS.[22]

Privacy Compliance Review

USCIS published a PIA for the National Appointment Scheduling System (NASS)[23] earlier in 2015. Due to the extensive amount of biometric information collected, stored, and shared by USCIS as part of the benefit application process (as detailed by the NASS PIA and this CPMS PIA), the DHS Privacy Office will begin a Privacy Compliance Review on the ASC biometrics collection, storage, and sharing process, including both CPMS and NASS and as appropriate, IDENT, within a 6 months of publishing this PIA.

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 legal authority to collect biometric and associated biographic information, including SSN, comes from 8 U.S.C. § 1101 *et seq.*

Section 103(a) of the Immigration and Nationality Act (INA) sets forth the Secretary of Homeland Security's authority to administer and enforce the immigration and naturalization laws.[24] In particular, under section 103(a)(3) of the INA, the Secretary of Homeland Security is authorized to prescribe forms, issue instructions, and perform other acts as deemed necessary to carry out his authority under the INA. DHS regulations at 8 CFR § 103.16(a) provide that any individual may be required to submit biometric information if the regulations or form instructions require this information or if requested in accordance with 8 CFR § 103.2(b)(9). Also, DHS is authorized under 8 CFR § 103.16(a) to use the biometric information collected to conduct background and security checks, adjudicate immigration and naturalization benefits, and perform other functions related to administering and enforcing the immigration and naturalization laws. DHS regulations at 8 CFR § 103.2(b)(9) provide that any applicant, petition, or any other individual may be required to appear for fingerprinting or an interview. As described in 8 CFR § 103.16(a), the more specific authority to conduct background checks through fingerprint and photograph collection is identified in regulations governing the particular benefit being requested.

[21] OBIM Information Sharing and Reporting Branch has access to CPMS via PCQS to support research and intelligence reporting functions.
[22] Although ICE and CBP have direct access to CPMS, ICE and CBP users may access data from CPMS and other USCIS systems through PCQS rather than accessing each system individually.
[23] *See* DHS/USCIS/PIA-057 National Appointment Scheduling System (NASS), *available at* www.dhs.gov/privacy.
[24] 8 U.S.C. § 1103(a).

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

The collection, use, maintenance, and dissemination of information is covered under DHS/USCIS-002 Background Check Service[25] and DHS/USCIS-003 Biometric Storage Systems SORNs.[26]

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

Yes. USCIS issued CPMS its Authority to Operate (ATO) on October 31, 2014, and is part of an Ongoing Authorization program. As such, CPMS will have an ongoing ATO with no expiration date.

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

The records 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.

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.

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, IVT is subject to the requirements set forth by PRA. Form M-1061 (OMB Control Number 1615-0125), which is an informational flyer, covers the biometric collection through IVT.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

CPMS collects, maintains, and disseminates the following information:

[25] *See* DHS/USCIS-002 Background Check Service, 72 FR 31082 (June 5, 2007).
[26] *See* DHS/USCIS-003 Biometric Storage System, 72 FR 17172 (Apr. 6, 2007).

- **Individual**: A-Number, date of birth, receipt number, full name, address, SSN, phone number, and other unique identifiers (e.g., T-Number);[27]
- **Immigration Information**: Type of application, country of birth, document issuance data;
- **Demographic Data**: Includes the collection of race, ethnicity, height, weight, eye color, and hair color;
- **Biometrics**: Includes biometric images (i.e., press-print, photograph, and signature) and details about those images (e.g., capture date);
- **Background Check information**: Includes results of the FBI name check, Universal Control Number (UCN),[28] FBI fingerprint check, DHS IDENT checks, and in some cases, DoD fingerprint check;
- **Encounter Data**: Includes transaction identifier data (sending organization; timestamp; ASC employee ID, workstation; and reason fingerprinted, including IDENT-generated EID); and
- **Card Data**: Includes details about cards issued for approved applications such as card serial number, Radio Frequency Identification (RFID) data associated with the Employment Authorization Document and the Permanent Resident Card, production site, production status, and time/date stamp of cards.

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

USCIS collects biometric information directly from benefit requestors to conduct background checks, including an IDENT verification check. CPMS centrally stores the photo, press-print, signature, and biographic and biometric data initially captured at an authorized fingerprint site for an individual applying for immigration-related benefits. The responses from the FBI and DoD background checks are stored in CPMS. Once adjudicated, CPMS receives and stores card and travel document production information after they are produced by the ICPS, TDPS, or EPMS. This information is received daily via the USCIS ESB. CPMS also receives information from various USCIS source systems.

[27] A T-Number is a temporary ID number used when no other identifying number is provided.
[28] The FBI Number is now called the Universal Control Number (UCN). The UCN is unique to the fingerprint identity, and all submissions for the same person will be associated with the same UCN. NGI issues a UCN for all biometric identities retained within NGI, not just those with criminal histories. Individuals without an FBI Number will receive a UCN. Individuals who currently have an FBI Number will retain that number as their UCN.

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

No.

2.4 Discuss how accuracy of the data is ensured.

USCIS ensures data accuracy by collecting biographic and biometric information directly from the benefit requestor or his or her representative. USCIS also biometrically verifies the accuracy of the information provided through the background check process. Biometric verification is an identity authentication process used to confirm a claimed identity through uniquely identifiable biological traits.[29]

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk to data minimization posed by maintaining the data in multiple systems.

Mitigation: CPMS facilitates biometrics-based identity verification. To enhance the integrity of the immigration system and combat identity fraud, USCIS collects biographic and biometric data to verify a customer's identity. USCIS biometric collection is limited to 10-prints (to support background checks) and document images (facial photo, signature, and single press-print to support document production). CPMS serves as the centralized repository for all biometric data captured by USCIS from applicants filing immigration applications. The consolidation of identity information (i.e., biographic and biometrics) allows USCIS to manage applicant identities, to include background checks, re-checks, and card production.

After CPMS captures fingerprints, they are transmitted to IDENT with associated biographic information for matching. USCIS searches and enrolls data in IDENT to establish and verify the identities of individuals applying for immigration benefits. A subset of information collected through CPMS is shared and stored in IDENT. OBIM's mission is to match, store, and share biometrics IDENT stores and processes biometric data, i.e., digital fingerprints and photographs, and links biometrics with biographic information to establish and verify identities. This reduces the possibility of identity theft and the risk of fraud by allowing USCIS adjudicators to verify visually the applicant presenting the biometrics with the identity already on file.

[29] Biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. Fingerprints, DNA, and signature are considered unique identifiers.

Privacy Risk: There is a risk of inaccurate data within CPMS because CPMS may not receive refreshed information from another USCIS system.

Mitigation: USCIS has not mitigated this risk. If a benefit requestor updates or changes his or her information after the card is produced, CPMS will not receive the update from the case management system. If the information is updated in CLAIMS 3 prior to card production, CPMS will receive the update. If the information is updated in BBSS before card production, but after the original data was sent to CLAIMS 3, CPMS will not receive the update. This is a USCIS-wide problem, not specific to CPMS.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

USCIS developed CPMS to be the centralized repository for USCIS biometric information. USCIS uses CPMS to store biometrics captured by USCIS used for biometric-based background checks, store image sets for benefit card and document production, and facilitate biometric-based identity verification. USCIS stores all biometric data and the biographical information required for FBI checks and card production within CPMS.

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.

No.

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

Yes. USCIS provides ICE, CBP, and OBIM access to CPMS either through a direct interface or via PCQS. CBP officers use CPMS data to validate the authenticity of immigration credentials (i.e., visas, passports, and permanent resident cards) presented to them during secondary inspections. ICE Immigration Enforcement Agents and Deportation Officers use CPMS data to obtain and verify information while investigating individuals who are suspected of violating immigration laws as well as violating federal criminal statutes. OBIM accesses CPMS via PCQS to support its research and intelligence reporting functions.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that in the consolidation of multiple systems, an

individual's information may be incorrectly associated with another individual.

Mitigation: This risk is partially mitigated. USCIS created CPMS to improve the accuracy of biometric information received from individuals for verification purposes. CPMS consolidates information from multiple, disparate, systems into one centralized system. USCIS is working to consider the FIN when associating biometric records rather than names, dates of births, and A-Numbers in CPMS. Data consolidation allows for greater control over the security and management of data. Use of a biometric identifier, once confirmed, is less susceptible to the lexicon, linguistic, and phonetic challenges associated with biographic information that risk mis-association.

Privacy Risk: There is a risk that information stored in CPMS may be used for purposes outside of the original purpose for which it was collected or disseminated inappropriately.

Mitigation: To mitigate the privacy risk of unauthorized use, all users are required to sign a CPMS- or PCQS-specific Rules of Behavior indicating that they have read, understand, and agree to abide by the system policies, before the supervisor and Accounts Management Branch authorizes access to information and the information system. The Rules of Behavior describe the user's responsibilities and expected behavior with regard to information and information system usage. Only users who have a need to know the information in the system can gain access to CPMS, and their access to information contained within the system is restricted to what is necessary to perform specific job-related functions.

Furthermore, users receive training on how to use CPMS and restriction on sharing the information it contains. All users' actions are recorded and periodically audited by program management. Despite the read-only nature of CPMS that limits electronic dissemination; there is the possibility that users can store/disseminate the information outside of the built-in safeguards (i.e., screen captures or screen prints). Users have all been informed that inappropriate use of the system or information contained therein could lead to reprimands and job loss. All users also receive training on the proper handling of information in accordance with laws, regulations, and policy, including but not limited to the Privacy Act.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

USCIS benefit applications and petitions require that biographic information be provided and some may also require the submission of fingerprints and photographs. The instructions for

certain forms notify the individual that biometric collection is required for the purpose of conducting background checks. Further, the instructions also advise the individual that the information is critical in making an informed adjudication decision in granting or denying a USCIS benefit and that the failure to submit such information may prohibit USCIS from processing and properly adjudicating the form and thus preclude the benefit requestor from receiving the benefit.

USCIS also provides general notice to individuals through the DHS/USCIS-003 Biometric Storage System SORN and this PIA. Further, USCIS presents all individuals seeking immigration benefits with a Privacy Act Statement as required by Section (e)(3) of the Privacy Act of 1974. The Privacy Act Statement is located on each form's instructions. The Privacy Act Statement located on the instructions for each form notifies individuals of USCIS's authority to collect information, and the purposes, routine uses, and consequences of declining to provide the information to USCIS prior to the collection of information. Therefore, through the application process, individuals are provided notice of the use of the information for adjudication purposes, including background investigations. In addition, USCIS publishes information on its website about its fingerprinting requirements and process.[30]

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

Individuals who apply for USCIS benefits are presented with a Privacy Act Statement as required by Section (e)(3) of the Privacy Act and sign a release authorization on the benefit request. Individuals who provide biometrics through the IVT receive a separate Privacy Act Statement at the point of collection. The Privacy Act Statements detail the authority to collect the information requested. The forms also contain a provision by which a benefit requestor authorizes USCIS to release any information received from the benefit requestor as needed to determine eligibility for benefits. An individual may decline to provide his or her biometrics but is cautioned that failure to do so may make result in USCIS' inability to determine eligibility for the requested benefit.

4.3 Privacy Impact Analysis: Related to Notice

There is no privacy risk associated with notice because USCIS provides notice to individuals that his or her information will be shared with the DoD and the FBI through a Privacy Act Statement, this PIA, and the associated SORNs.

[30] http://www.uscis.gov/forms/fingerprints.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

The records will be retained for 100 years from the date of birth of the individual in accordance with NARA Disposition Authority Number DAA-0563-2013-0001-0005. The information is collected to support the maintenance of card issuances and the background check processes. CPMS maintains USCIS benefit applicant biometric images (photograph, fingerprint, and signature) and basic biographic data collected at USCIS offices.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is risk that information maintained by USCIS will become inaccurate and dated since it is retained for 100 years from the individual's date of birth.

Mitigation: Biographic and biometric information in CPMS is needed for the indicated time because the relationship between an applicant and USCIS may span the applicant's entire life. USCIS uses biometrics to verify the claimed identity through uniquely identifiable biological traits, which do not become inaccurate or untimely over time. USCIS also uses the historical data in CPMS in the adjudication of applications and petitions. The biometric records mirror the retention schedule of the A-File. The A-File is the physical paper file containing all correspondence and documentation, including all applications, petitions, reports, interview notes, and other written communications for every applicant. The A-File records are permanent, whether hard copy or electronic. USCIS transfers the A-Files to the custody of NARA 100 years after the individual's date of birth.

Privacy Risk: There is privacy risk that CPMS information is retained longer than required, increasing the opportunity for unauthorized disclosure and corruption of the data.

Mitigation: This risk is partially mitigated. Although there is always an inherent risk in retaining information for any length of time, the CPMS information retention periods are consistent with the concept of retaining information only for as long as necessary to support the agency's mission. If an individual does not become a naturalized citizen, he or she may continue to interact with USCIS throughout his or her life. The System Administrator is responsible for reviewing, deleting, or archiving information in accordance with the retention schedule. Also, security controls are in place to ensure that information is protected during this time.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

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.

Yes. USCIS shares information maintained in CPMS with the Department of State (DoS), the Department of Justice (DOJ) Federal Bureau of Investigation (FBI), and the Department of Defense (DoD).

Department of State

USCIS provides the DoS Bureau of Consular Affairs read-only access to CPMS for visa and passport adjudication responsibilities, as well as fraud detection and investigation responsibilities. CPMS data is accessed by DoS Bureau of Consular Affairs through the use of PCQS. The DoS user community does not have direct access to CPMS. All access controls and identification and authentication are external to CPMS and under the control of PCQS.[31]

Department of Justice Federal Bureau of Investigation

USCIS sends benefit requestor information (i.e., name, A-Number or SSN, date of birth, country of birth, race, gender, physical characteristics, address, reason for fingerprint, and fingerprint and facial photo images) to the FBI to conduct the name and fingerprint checks. The FBI responds to the FBI Name and/or Fingerprint Check with either a: "no record," "positive response," or "pending." A no record response means that the FBI has no relevant information on benefit requestor. A pending response means further research is needed before the FBI can provide a final response. For those records with an initial response of pending, the FBI completes a review of their records and provides a final response of no record or positive response. A positive response means the FBI has information relating to the individual. All FBI Name and Fingerprint Check requests, responses, and queries flow through the ESB; there is no direct connection between the FBI's respective systems and CPMS.

[31] *See* DHS/USCIS/PIA-010 Person Centric Query Service (PCQS), *available at* www.dhs.gov/privacy.

Department of Defense (DoD)

USCIS uses LiveScan to capture biographic and biometric information for applicants seeking immigration benefits from USCIS. CPMS via the ESB sends benefit requestor's name, A-Number, date of birth, country of birth, race, gender, physical characteristics, address, reason for fingerprint, and fingerprint & facial photo images to DoD for a fingerprint check fingerprint on specific refugee and asylum filing types. DoD responds to the Fingerprint Check with either a: "Non-Match" or "Match." A Non-Match response means that DoD has no relevant information based on the fingerprints of the benefit requestor. An IDENT response means there is a matching in the military encounter database. All DoD Fingerprint Check requests, responses, and queries flow a direct connection between DoD's ABIS processing and CPMS via ESB.

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

Sharing USCIS CPMS data with DoS is compatible with the purpose of the system because the DoS mission, like USCIS, includes ensuring lawful visits and immigration to the United States as dictated by the INA. The external sharing of biographic and biometric information with DoS is covered under Routine Use C of the DHS/USCIS-003 Biometric Storage System, which allows USCIS to share information in CPMS with DoS to assist in the processing of petitions or applications for benefits under the Immigration and Nationality Act, which is the purpose for which USCIS collected the biometrics.

Sharing USCIS CPMS data with FBI and DoD is compatible with the purpose of the system because USCIS is required to conduct background and security checks to identify threats to national security and public safety posed by those seeking immigration benefits. The external sharing of biographic information with the FBI and DoD is covered under routine use G of the DHS/USCIS-002 Biometric Check System, which allows USCIS to share information in CPMS with FBI and DoD to verify the applicant's eligibility for the benefit being sought.

6.3 Does the project place limitations on re-dissemination?

Yes. A Memorandum of Understanding (MOU) exists between DHS and DoS that covers the sharing of immigration benefit records. The MOU describes policies and procedures to prevent unauthorized dissemination of information. Additionally, the MOU clarifies the authority for DoS and DHS to share immigration and naturalization records and the basic mechanisms established to protect this data.

DoS users must sign an agreement to acknowledge that they will abide by all DHS policies and regulations concerning the security of the data delivered. External users viewing biographic and biometric information via the CPMS or PCQS must adhere to the system Rules of Behavior. The Rules of Behavior explicitly state that the data may not be shared with any other user, and that the data may not be stored on any device.

DHS has signed separate MOUs with the FBI and DoD that set forth the terms and conditions for the transfer and use of information pertaining to biographic and biometric background checks. FBI and DoD employees who perform background checks have received the required training to perform the checks. In addition, the FBI and DoD have policies and procedures in place to ensure that information is appropriately disseminated.

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

USCIS maintains audit logs to identify transactions performed by ESB and PCQS. Logs are created for every transaction in CPMS. Each audit log contains User ID, date of event, time of event, type of event (login, logout, query), and description (i.e., what information was searched and returned and a reference to location of database searched).

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: The primary privacy risk associated with external information sharing is the potential disclosure of data for purposes that are not in accord with the stated purpose and use of the original collection.

Mitigation: This privacy risk is partially mitigated by comparing disclosures to the routine uses of the SORNs listed in 1.2. DHS has MOUs in place with DoS, DoD, and FBI to ensure that there are formal procedures in place to secure and protect biographic and biometric information. As discussed above, CPMS maintains a record of disclosure of information in accordance with the routine use or with which it has an information sharing agreement. A record is kept as system audit trail logs, which are maintained to identify transactions performed by users. DoS, DoD, and FBI employees have received the required training to access these systems. DoS, DoD, and FBI employees are trained and authorized to handle biographic and biometric data. In addition, DoS, DoD, and FBI have policies and procedures in place to ensure that information is not inappropriately disseminated.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

An individual seeking access to his or her information may gain access to their USCIS records by filing a Freedom of Information Act (FOIA) or Privacy Act request and submitting the requests to following address:

USCIS National Records Center
Freedom of Information Act/Privacy Act Program
P.O. Box 648010
Lee's Summit, MO 64064-8010

Further information for Privacy Act and FOIA requests for USCIS records can also be found at http://www.uscis.gov.

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

Individuals may direct all requests to contest or amend information to the USCIS FOIA/PA Office. Individuals must state clearly and concisely in the redress request the information being contested, the reason for contesting it, the proposed amendment, and clearly mark the envelope "Privacy Act Amendment."

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

Individuals are notified about procedures for correcting their information by relevant USCIS application instructions, the USCIS website, this PIA, and relevant SORNs.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that USCIS may not afford the individual adequate opportunity to correct data maintained in CPMS.

Mitigation: Information in CPMS is derived from other USCIS systems and there is a process to update records during the adjudication process. During the adjudication process, an officer may request a data edit. Individuals are given numerous opportunities during and after the completion of the benefit request process to correct information they have provided and to respond to information received from other sources. If a data correction to CPMS is deemed necessary, the officer submits a G-1273 Data Edit request form to the Biometrics Division, which then makes the necessary update to the CPMS database. USCIS does not claim any Privacy Act exemptions for CPMS and therefore individuals may submit a redress request as stated in the applicable SORN.

Privacy Risk: There is risk of USCIS denying a benefit based on inaccurate data received from DOJ or DoD and not affording the individual to correct data provided by the background check.

Mitigation: The facilitation of FBI and DoD background checks is a required part of the adjudication process, which must occur prior to granting a benefit. USCIS mitigates this risk by providing the benefit requestor with the opportunity to explain and or provide additional documentary evidence to resolve any concerns prior to issuing a final decision. If USCIS

identifies derogatory information, USCIS issues a Request for Evidence or a Notice of Intent to Deny directly to the benefit requestor. Additionally, if there is a criminal record, USCIS verifies the accuracy of the information with the state and local law enforcement source before an adverse decision is finalized. The ISO evaluates and makes a final decision based on the totality of the circumstances.

Section 8.0 Auditing and Accountability

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

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

USCIS ensures that the practices stated in this PIA are followed by using training, policies, information sharing access agreements, Rules of Behavior, and auditing. All USCIS systems employ auditing measures and technical safeguards to prevent the misuse of data. Access and security controls have been established to mitigate privacy risks associated with authorized and unauthorized users, namely misuse, and inappropriate dissemination of data. DHS security specifications require auditing capabilities that log the activity of each user in order to reduce the possibility of misuse and inappropriate dissemination of information. In accordance with DHS security guidelines, USCIS systems use auditing capabilities that log user activity. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

CPMS users receive training on how to use CPMS and restrictions associated with sharing the information it contains. In addition, all USCIS employees and contractors are required to complete the annual privacy and security awareness training to ensure their understanding of properly handling and securing PII. The Privacy Awareness training addresses appropriate privacy concerns, including Privacy Act obligations (e.g., SORNs, Privacy Act Statements). The Computer Security Awareness training examines appropriate technical, physical, personnel, and administrative controls to safeguard information.

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

CPMS implements role-based access controls leveraged from USCIS Active Directory services. Specific user group templates are utilized to detail the level of privileges for each

CPMS user group. Users are only given access to system information for which they have a need-to-know. The need-to-know is determined by the employee's supervisor. Access control policies and associated access enforcement mechanisms (e.g., access control lists and access control matrices are employed to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) on the CPMS system. Access to the server security functions (e.g., audit trails, access control lists, and password files) is explicitly restricted to system administrators; database functions are explicitly restricted to database administrators.

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?

USCIS has a formal review and approval process in place for new sharing agreements. Any new use of information or new access requests for the system must go through the USCIS change control process and must be approved by the proper authorities of this process such as the USCIS Privacy Officer, Chief of Information Security Officer, Office of Chief Counsel, and the respective Program Office.

Responsible Officials

Donald Hawkins
Privacy Officer
United States Citizenship and Immigration Services
Department of Homeland Security

Approval Signature

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

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security