Privacy Impact Assessment Update
for the

Customer Profile Management System

DHS/USCIS/PIA-060(b)

August 14, 2018

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

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The U.S. Citizenship and Immigration Services (USCIS) Customer Profile Management Service (CPMS) serves as a person-centric repository of biometric and biographic information provided by applicants and petitioners (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, or travel documents). USCIS is updating this Privacy Impact Assessment (PIA) to account for CPMS ingesting historical Federal Bureau of Investigation (FBI) name check records, modernizing the name check process, adding a new system interconnection to the Person Centric System, and migrating to a cloud-hosted environment.

Overview

USCIS oversees lawful immigration to the United States and 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; (2) verify a 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) serve as the centralized repository of biometrics captured by USCIS; (2) serve as the centralized authoritative source of image sets for benefit card and document production; (3) facilitate identity verification; (4) conduct criminal and national security background checks against DHS and non-DHS systems, and (5) support domestic and foreign data sharing. CPMS enhances USCIS's mission by consolidating biometric and biographic data in a centralized, person-centric, searchable repository.

Reason for the PIA Update

USCIS is submitting this PIA to account for the following updates:

Modernized FBI Name Check Request Process

All individuals seeking a U.S. immigration benefit are subject to criminal and national security background checks to ensure they are eligible for that benefit. USCIS conducts security

checks for all cases involving a benefit request form for an immigration service or benefit. This is done both to enhance national security and ensure the integrity of the immigration process. The CPMS PIA published on December 17, 2015, accounts for FBI name checks as part of the security and background check process. However, this PIA Update describes the new module that allows USCIS employees to initiate and conduct FBI Name Checks through a user interface.

USCIS developed the CPMS Name Check (CPMS-NC) module as a long-term effort to modernize and retire the Benefits Fingerprint Processing Mainframe (FD-258 MF), the legacy name check application.[1] FBI name checks are required for many benefit request forms and USCIS conducts FBI name checks on applicants, petitioners, and beneficiaries seeking certain immigration benefits. CPMS-NC allows USCIS employees to initiate name check requests directly with the FBI through the FBI's Next Generation Name Check Program (NGNCP).[2] Name checks are conducted using information provided on the benefit request form. The FBI Name Check responses are used to determine whether an individual has a record that might have an impact on the individual's eligibility for the benefit sought.

USCIS employees initiate an FBI Name Check using the individual's full name or a personal identifier (i.e., Alien Number, Receipt Number, Social Security number) directly with the FBI through the CPMS-NC. Before routing a request, CPMS-NC is able to detect the existence of duplicate submissions (i.e., identically spelled names with identical dates of birth submitted within the last 60 days) and is able to quickly refer the USCIS employee to the previous response, which is intended to improve processing times at the FBI as it lowers the amount of time spent processing and deconflicting duplicates. Duplicate submissions were previously submitted to the FBI and any duplicate findings were returned immediately to USCIS. If there are no duplicate submissions detected, CPMS forwards the name check request to the FBI along with the individual's name, date of birth, country of birth, race, and gender to the FBI to conduct a name check.

The FBI Name Check consists of name-based manual and electronic searches of the FBI's Central Records System (CRS).[3] CRS contains personnel, administrative, applicant, intelligence, and criminal files that have been compiled for law enforcement purposes. The FBI searches seek all instances of the individual's name appearing in the CRS files, and FBI staff then review and analyze potential identifiable documents to determine whether a specific individual has been the subject of or been mentioned in any FBI investigation(s), and if so, whether relevant information, if any, may be disseminated to the requesting agency.

The FBI responds to each FBI Name Check with a: "no record," "positive response," or "pending." A "no record" indicates that the FBI's records contain no identifiable information regarding a particular individual. A pending response means further research is needed before the

[1] The FD-258 Mainframe application was decommissioned on March 31, 2018.
[2] https://www.fbi.gov/services/records-management/name-checks.
[3] See DOJ/FBI-002 Central Records System (CRS), 82 FR 24147 (May 25, 2017).

FBI can provide a final response. If a match was identified, then the FBI forwards a summary, known as a Letterhead Memorandum (LHM), of the reportable information to USCIS. Responses are stored in CPMS.

Ingestion of Historical FBI Name Check Records

USCIS shut down several mainframe applications to modernize the current systems managed by and operated on mainframes, including FD-258 MF. USCIS recently dispositioned FD-258 MF, the legacy name check system, and migrated the FD-258 MF functionality and name check records to CPMS. All historical name checks results and unclassified LHMs have been migrated to CPMS for historical purposes. LHM data includes biographic data, name check transmission data, and name check response data. These records are stored to assist in the adjudication process. Through CPMS-NC, USCIS employees are able to access and retrieve historical name check records. USCIS employees with access to CPMS-NC may search an individual's name check history with an A-Number with optional date of birth or date of birth range; receipt number; or a combination of names and biographical information.

Person Centric System (PCS) Interconnection

In the past, USCIS used several legacy case management and other record systems to administer and adjudicate immigration benefits and services. Each disparate system uniquely maintained independent records on an individual involved in a benefit or service request. USCIS systems did not provide a holistic view of an individual person or what actions the agency has taken with respect to that person. The lack of a consolidated, cohesive, and historic view of individuals engaging with USCIS resulted in several privacy risks, such as duplicative and inaccurate records.

USCIS is developing PCS to move towards the person-centric approach. PCS will be either one system composed of multiple microservices, or multiple new microservices integrated with existing systems to support person-centric services. USCIS plans to consolidate information about customers in one central system or one queryable index. These proposed person-centric services are being called PCS.

PCS will be developed in incremental phases using the agile approach.[4] PCS plans to retrieve and store CPMS data to support the various PCS microservices and functions. Various PCS microservices may use the different combinations of data elements from CPMS for separate purposes. For instance, the A-number validation microservice uses the following data elements:

- A-Number
- Social Security number (SSN)

[4] At the time of publication, there are two microservices operating as part of PCS–the A-number validation service, and an entity resolution service.

- Receipt Number
- Fingerprint Identification Number
- Full Name
- Date of Birth
- Country of Birth
- Country of Citizenship

The list of data elements above is not a comprehensive list of CPMS data shared with PCS. The PCS microservices are intended to enhance existing processes by associating data from USCIS systems, including CPMS, DHS systems, and non-DHS source systems, performing data analysis using the associated data, and managing and resolving identities across systems. As PCS and its microservices are deployed, USCIS will issue updates to the PCS PIA to outline the CPMS data retrieved and used by PCS and its microservices.[5]

Migration to Cloud-based Platform

As noted above, USCIS is undergoing a legacy system modernization effort to align with the "Cloud First" policy in order to improve business operations.[6] When evaluating options for new IT deployments, the Office of Management and Budget (OMB) requires that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. USCIS migrated CPMS to the Amazon Web Services (AWS) cloud platform. This migration does not impact the collection and use of personally identifiable information (PII) in CPMS. USCIS requires AWS to segregate CPMS data from all other third-party data. The cloud-hosted CPMS functionality and interfaces remains intact. All existing records from CPMS were extracted from the legacy database and transferred to the new cloud environment. This technological advancement does not impact the collection and use of records in CPMS, but modifies the way USCIS stores and maintains CPMS records.

Privacy Impact Analysis

Authorities and Other Requirements

The legal authority to collect biometric and associated biographic information, including SSN, does not change with this update. The legal authority to collect biometric and associated biographic information, including SSN, comes from 8 U.S.C. § 1101 et seq.

[5] At the time of publication of this PIA, the PCS PIA had not yet been completed.
[6] *See* "25 Point Implementation Plan to Reform Federal Information Technology Management" (December 9, 2010), *available at* https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf.

The collection, use, maintenance, and dissemination of information are covered under the DHS/USCIS-018 Immigration Biometric and Background Check System of Record SORN.[7]

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 (PRA) 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.

Characterization of the Information

This update does not impact the collection of information in CPMS. USCIS continues to collect and maintain the information outlined in Section 2.0 of the DHS/USCIS/PIA-060 CPMS. The new CPMS-NC module and migration of historical name check records from FD-258 does not introduce a new collection of information. Also, the PCS interconnection only retrieves information from CPMS. No information from PCS is shared with CPMS.

Uses of the Information

The introduction of the CPMS-NC module, the migration of historical name check records from FD-258, PCS interconnection, and migration to the cloud do not introduce new uses of information. USCIS continues to use CPMS to: (1) serve as the centralized repository of biometrics captured by USCIS; (2) serve as the centralized authoritative source of image sets for benefit card and document production; (3) facilitate identity verification; (4) conduct criminal and national security background checks against DHS and non-DHS systems, and (5) to support domestic and foreign data sharing.

Notice

USCIS is providing general notice about the system changes through this PIA update. USCIS is also publishing DHS/USCIS-018 Immigration Biometric and Background Check System of Record SORN to provide additional transparency about the biometric check, biographic background check, identity verification and resolution, card production record systems, and data

[7] DHS/USCIS-002 Background Check Service, 72 FR 31082 (June 5, 2007) and DHS/USCIS-003 Biometric Storage System, 72 FR 17172 (Apr. 6, 2007) are in the process of being combined and reissued as one SORN.

sharing efforts. The Privacy Notice located on the instructions for each form notifies individuals of USCIS's authority to collect information, the purposes of the collection, routine uses of the information, and consequences of declining to provide the information to USCIS. 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.

Privacy Risk: There is a privacy risk that individuals providing information to USCIS do not receive sufficient notice that explains their information is being stored on a server not owned or controlled by USCIS.

Mitigation: This risk is partially mitigated. This PIA provides notice that information is stored in a cloud-based system, and USCIS provides general notice to individuals about the collection and use of their information. USCIS, however, does not provide explicit notice at the time of collection that the information may be stored in a cloud-based system. Regardless of storage location of records, CPMS records are governed by USCIS's collection, use, and dissemination of personally identifiable information.

Data Retention by the project

This update does not impact the retention of information in CPMS. The records will continue to 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 creation and issuance of cards and the background check processes.

Information Sharing

Modernized FBI Name Check Request Process

CPMS-NC replaces the legacy FBI name check process.[8] USCIS uses CPMS-NC module to securely connect to FBI NGNCP to initiate a FBI Name Check. CPMS sends benefit requestor or beneficiary information, to include name, date of birth, country of birth, race, and gender to the FBI to conduct a name check. The NGNCP conducts manual and electronic searches of the FBI's CRS. The CRS encompasses the centralized records of FBI Headquarters, field offices, and legal attaché offices, as well as all investigative, administrative, personnel, and general files. Since the use of CRS was previously described in the CPMS PIA, published on December 17, 2015, there are no new risks associated with the sharing of information with the FBI to conduct name checks.[9]

[8] S*ee* DHS/USCIS/PIA-060 Customer Profile Management Service *available at* www.dhs.gov/privacy.
[9] S*ee* DHS/USCIS/PIA-060 Customer Profile Management Service *available at* www.dhs.gov/privacy.

Ingestion of Historical FBI Name Check Records

There are no impacts to information sharing with the migration of historical fingerprint records to CPMS from FD-258 MF. The CPMS PIA, published on December 17, 2015, covers the maintenance of FBI Name Check results.[10] There are no new risks associated with the ingestion of historical FBI Name Check Records in CPMS.

PCS Interconnection

The use of CPMS records by PCS does not impact information sharing. CPMS data was previously shared with internal USCIS systems to support identity verification initiatives. There are no new risks with the use of CPMS records by PCS. The use and sharing of information will be discussed in the PCS PIA.

Migration to Cloud-based Platform

USCIS migrated the CPMS to AWS cloud platform. This migration does not impact information sharing practices in CPMS from the previous legacy system. USCIS requires AWS to segregate CPMS data from all other third-party data. The cloud-hosted CPMS system absorbed legacy CPMS functionality and system interconnections.

Redress

This update does not impact how access, redress, and correction may be sought through USCIS. USCIS continues to provide individuals with access to their information through a Privacy Act or Freedom of Information Act (FOIA) request. Individuals 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. U.S. Citizens and Lawful Permanent Residents may also file a Privacy Act request to access their information. If an individual would like to file a Privacy Act or FOIA request to view his or her USCIS record, the request can be mailed to the following address:

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

Persons not covered by the Privacy Act or JRA are not able to amend their records through FOIA. Should a non-U.S. person find 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.

[10] S*ee* DHS/USCIS/PIA-060 Customer Profile Management Service *available at* www.dhs.gov/privacy.

Auditing and Accountability

USCIS ensures that practices stated in this PIA comply with federal, DHS, and USCIS standards, policies, and procedures, including standard operating procedures, rules of behavior, and auditing and accountability procedures. CPMS is maintained in the AWS, which is a public cloud designed to meet a wide range of security and privacy requirements (e.g., administrative, operational, and technical controls) that are used by USCIS to protect data in accordance with federal security guidelines.[11] AWS is Federal Risk and Authorization Management Program (FedRAMP)-approved and authorized to host PII.[12] FedRAMP is a U.S. government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud services.

USCIS employs technical and security controls to preserve the confidentiality, integrity, and availability of the data, which are validated during the security authorization process. These technical and security controls limit access to USCIS users and mitigates privacy risks associated with unauthorized access and disclosure to non-USCIS users. Further DHS security specifications also require auditing capabilities that log the activity of each user in order to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify information by user identification, network terminal identification, date, time, and data accessed. All USCIS systems employ auditing measures and technical safeguards to prevent the misuse of data.

Privacy Risk: The data maintained by Amazon Web Services (AWS) for the purposes of cloud hosting may be vulnerable to breach because security controls may not meet system security levels required by DHS.

Mitigation: This risk is mitigated. USCIS is responsible for all PII associated with the CPMS system, whether on USCIS infrastructure or on a vendor's infrastructure, and it therefore imposes strict requirements on vendors for safeguarding PII data. This includes adherence to the DHS 4300A Sensitive Systems Handbook, which provides implementation criteria for the rigorous requirements mandated by DHS's Information Security Program.[13] USCIS cloud service providers must be FedRAMP-certified. By using FedRAMP-certified providers, USCIS leverages cloud services assessed and granted provisional security authorization through the FedRAMP process to increase efficiency while ensuring security compliance. All contracted cloud service providers must follow DHS privacy and security policy requirements. Before using AWS, USCIS verified through a risk assessment that AWS met all DHS privacy and security policy requirements. Further, all cloud-based systems and service providers are added to the USCIS Federal Information

[11] Public clouds are owned and operated by third-party service providers whereas private clouds are those that are built exclusively for an individual enterprise.
[12] https://marketplace.fedramp.gov/#/product/aws-us-eastwest?status=Compliant&sort=productName.
[13] *See* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

Security Modernization Act (FISMA) inventory and are required to undergo a complete security authorization review to ensure security and privacy compliance. As part of this process, the DHS Senior Agency Official for Privacy reviews all FedRAMP cloud service providers for privacy compliance and privacy controls assessments as part of the privacy compliance review process.

Responsible Officials

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.

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security