# Privacy Impact Assessment Update

**for the**

# Customer Profile Management System

**DHS Reference No. DHS/USCIS/PIA-060(c)**

**May 3, 2024**

Homeland Security

## Abstract

The Department of Homeland Security (DHS) U.S. Citizenship and Immigration Services (USCIS) Customer Profile Management Service (CPMS) serves as a person-centric repository of biometric and associated biographic information provided by applicants, petitioners, requestors, and beneficiaries (hereafter collectively referred to as "benefit requestors") who are issued a secure card or travel document identifying the receipt of an immigration benefit. This Privacy Impact Assessment (PIA) update discusses the deployment of CPMS 2.0, the removal of LiveScan (third-party software), the implementation of Biometric Enrollment Tool (BET) and its potential use by Foreign Service Nationals (FSN), the modernization of the CPMS Data Change Delete Request Form G-1273, and other CPMS interconnections with ATLAS (not an acronym); Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR); Global (not an acronym); Standard Management Analysis Reporting Tool (SMART); Content Management Services (CMS); and the Person Centric Identity Service (PCIS).

## Overview

USCIS oversees lawful immigration to the United States and receives and adjudicates requests for immigration benefits. USCIS captures biographic and biometric data from benefit requestors to facilitate the following operational functions: (1) conduct name and fingerprint-based background checks; (2) verify a benefit requestor's identity; and (3) store benefit card/document data and serve as the centralized authoritative source of image sets for benefit card and document production. 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.

Accordingly, USCIS implemented the CPMS to centralize and improve the collection and maintenance of biometric and biographic data into a single repository. The overall purpose of CPMS is to serve as a person-centric repository of all biometric and biographic data provided by benefit requestors. This system ingests, captures biometrics for identify verification, and maintains all biometric data in other USCIS systems, as well as stores benefit cards issued to non-U.S. citizens, facilitates criminal and national security background checks, and supports domestic and foreign data sharing. Its key functionality includes the following:

1. Provide query capabilities to search and locate biometric data;
2. Support information sharing where a biometric is the primary data element; and
3. Facilitate the use of the information for biometric-based identity verifications and background checks.

The primary function of CPMS is to provide USCIS with the capability to maintain and

use biometric images and biographic information of USCIS benefit requestors in support of their benefits requests. This allows USCIS to maintain a person-centric view of interactions between an individual and USCIS, rather than access disparate systems individually to view these interactions.

## Reason for the PIA Update

USCIS is updating the CPMS Privacy Impact Assessment to discuss the deployment of CPMS 2.0, the removal of LiveScan (third-party software), the implementation of the Biometric Enrollment Tool[1] and the potential use by Foreign Service Nationals,[2] and the modernization of the CPMS Data Change/Delete/Request Form G-1273. This Privacy Impact Assessment update also identifies and discusses the internal USCIS interconnections with the following systems related to encounter events[3] with applicants, petitioners, beneficiaries:

- ATLAS[4] (not an acronym), is a fraud detection application utilized by USCIS Fraud Detection National Security (FDNS) for security screening and vetting for fraud and egregious criminal activity. CPMS uses encounter data to detect potential derogatory information related to national security, public safety, and fraud and support accurate exchange of data among USCIS, DHS, and non-DHS systems;
- Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR),[5] which stores CPMS data to support agency data management and reporting efforts;

[1] The Biometric Enrollment Tool is used to electronically collect biometric information (fingerprints) from applicants and their beneficiaries seeking immigration benefits.
[2] Foreign Service Nationals are locally engaged staff hired under local compensation plans at a U.S. mission abroad under Chief of Mission authority. USCIS employs Foreign Service Nationals under Department of State Personal Services Agreements. The Department of State conducts background checks for all Foreign Service Nationals employed at USCIS international offices, and USCIS confirms that the Department of State background checks have been completed and are current, conducts its own additional personnel checks, and certifies all mandatory ethics and privacy training has been completed. All Foreign Service Nationals employed at USCIS international offices are supervised by U.S. citizen federal employees.
[3] Encounters are events that occur when USCIS or contract staff interact with an applicant/benefit requestor, including appointments at USCIS Application Support Centers to have their biometrics captured to support USCIS adjudications.
[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR ATLAS (DHS/USCIS/PIA-084), *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[5] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR ENTERPRISE CITIZENSHIP AND IMMIGRATION SERVICES CENTRALIZED OPERATIONAL REPOSITORY (eCISCOR) (DHS/USCIS/PIA-023), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

- Global[6] connects with CPMS to review background check information on benefit requestors;
- Standard Management Analysis Reporting Tool (SMART)[7] provides CPMS data to generate and reconcile Application Support Center (ASC) reports, CPMS connects with Content Management Services (CMS)[8] to access Federal Bureau of Investigation (FBI) "hits" and their corresponding, unclassified Letterhead Memorandum (LHM); and
- Person Centric Identity Service (PCIS),[9] which supports background checks and identity services, and maintains encounter events and benefit requestor data.

The new interconnections with CPMS are discussed below.

***Implementation of Customer Profile Management Service 2.0 (CPMS 2.0)***

The implementation of the CPMS 2.0 application streamlines search functions to enhance CPMS's general use. The new application establishes a user interface that facilitates centralized storage of all record checks and related biometrics, establishing a platform to easily locate results of background checks. Search results display an "at-a-glance" view that highlights important record information and any discrepancies. The new version of the application enhances functionality for requesting corrective edits to CPMS Encounter Data and adds integrity to the revision process, which is validated within the application to check the end user's work. Further, the end user selects the appropriate encounter for editing within CPMS 2.0 and initiates the data revision without entering the data manually. CPMS no longer creates separate internal encounters when biometrics are reused. Instead CPMS 2.0 now associates reuse encounters with the initial encounters to establish the relationship between the two and displays the purpose of the reuse. This enhancement adds integrity to the data edit process by ensuring each encounter associated with the initial encounter displays the edits made to that record.

The new functionality streamlines business processes, improves data integrity, enables the validation of new values, and creates efficiencies throughout the edit process to facilitate the complete inclusion of data edits.

---

[6] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR ASYLUM DIVISION (DHS/USCIS/PIA-027(d) and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[7] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR STANDARD MANAGEMENT ANALYSIS REPORTING TOOL, (SMART) (DHS/USCIS/PIA-050), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[8] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR CONTENT MANAGEMENT SYSTEM (DHS/USCIS/PIA-079), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[9] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR PERSON CENTRIC IDENTITY SERVICE (PCIS) (DHS/USCIS/PIA-087), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

***Modernization of CPMS's Data Change Delete Request Form (G-1273)***

CPMS Form G-1273 utilized the Enterprise Collaboration Network (ECN)[10] SharePoint site that required users to identify themselves and their organizations when initiating a request. Previously, all data entry processes for Form G-1273 were manual and required approved users to search for and view CPMS Encounter Records. For values associated with applicant encounters, both the initial value(s) and new value(s) for an applicant encounter were required for each CPMS Encounter Record. Further, the requesting party (USCIS user) was required to provide details of where they performed their job duties, prior to submission, which would inform how the request was routed to the appropriate individual for review and approval or disapproval. Approved requests were manually entered into the CPMS database by developers on the CPMS support team.

Modernization of the manual process related to applicant encounters using the legacy G-1273 tool on the ECN SharePoint site resulted in the development of G-1273 Application (G-1273 App) data edit functionality within the CPMS application. The G-1273 Application data edit feature automates and enforces role-based access/permissions through the Identity, Credential, and Access Management (ICAM) system.[11] The new data edit process allows an end user to create a profile within the CPMS Application to rout the edit request to the person responsible for reviewing and approving the edit request within their respective user group. This group assignment happens once and is not repeated for each request. An end user may also select the appropriate encounter data for editing within CPMS 2.0 and initiate the data edit without manual data entry. The new functionality validates newly entered values, creates efficiencies throughout the edit process, and enforces completeness of data element submissions to enhance data integrity. Integrating the G-1273 Application with CPMS 2.0 ensures that all security requirements of the CPMS Authority to Operate (ATO) apply to the G-1273 Application, keeping Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII) secure. Furthermore, data edit workflow processes with the CPMS 2.0 application are enhanced and burden on development resources is reduced through automated database revisions, upon approval.

***Implementation of Biometrics Enrollment Tool (BET) Module***

USCIS employees and Foreign Service Nationals use USCIS Application Support Center (ASC) and Service Center (SC) workstations to collect from benefit requesters electronic fingerprints, photos, signatures, and fingerprints obtained via the Benefit Fingerprint Processing

[10] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR ENTERPRISE COLLABORATION NETWORK (ECN) (DHS/USCIS/PIA-083) and subsequent updates, *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[11] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE PERSONAL IDENTIFY VERIFICATION IDENTITY MANAGEMENT SYSTEM (PIV/IDMS), DHS/ALL/PIA-014 and subsequent updates, *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

Mainframe (FD-258) cards.[12] LiveScan, a third-party software, formerly installed on workstations or kiosks located at Application Support Centers and Service Centers, was decommissioned in November 2021. USCIS may use paper FD-258 cards to digitize inked prints using the Biometrics Enrollment Tool, which is a custom CPMS module used to capture biometric data (electronic fingerprints, photos, signatures) from benefit requestors to confirm the benefit requestor's identity and initiate background check processes. The information captured is sent to the Office of Biometric Identify Management's (OBIM) Automated Biometric Identification System (IDENT),[13] which will be replaced by the Homeland Advanced Recognition Technology system (HART),[14] to confirm and validate the identity of the benefit requestor by comparing fingerprint records. USCIS-approved users have user roles labeled "Biometric Machine Operators" and are only allowed specified biometrics capture access to the Biometrics Enrollment Tool. Approvals and authorizations for USCIS users (including Foreign Service Nationals) are provided by USCIS International Field Office Directors, who assign each employee's user role and levels of access as part of the user access approval workflow.

***Content Management Services (CMS)***

Content Management Services is a cloud-based platform developed by USCIS to manage immigration-related content which is accessed and retrieved through a user interface called STACKS[15] (not an acronym), or through separate USCIS interconnected systems. It serves as a core technical enhancement of the transformation initiative for the storage and management of electronic immigration-related content in support of intake, case adjudication, and records management. CPMS interconnects with Content Management Services to access FBI "hits" and their corresponding unclassified Letterhead Memorandum generated from the FBI response records through the Application Program Interface (API) residing in the Amazon Web Services (AWS) Cloud infrastructure. CPMS 2.0 uses the information obtained to provide results for CPMS – Name Check to determine whether a specific individual has been the subject of or mentioned in any FBI investigation(s), and if so, whether relevant information, if any, may be disseminated to

[12] The paper form (i.e., FD-258 cards) is used by USCIS to capture inked fingerprints for scanning into CPMS to initiate background checks. The paper form of the FD-258 is used in specific use cases when an applicant is medically unable to provide digital prints. After the inked prints are captured, the physical FD-258 card is scanned into CPMS creating a digitized record of the applicant's fingerprints.

[13] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-002 (2012), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

[14] *SEE* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART) INCREMENT 1, DHS/OBIM/PIA-004 (2020), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

[15] STACKS is a digital file viewing and content management system for official immigration records as part of the Content Management Services directly supporting transformation.

the requesting agency. The records are searched to determine whether an individual has a record that may have an impact on the individual's eligibility for the benefit sought. In most instances, applicable information found in the FBI's Name Check search will be returned as a Letterhead Memorandum[16] or a Report.

***Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR)***

The Enterprise Citizenship and Immigration Services Centralized Operational Repository was developed to consolidate and manage immigration and naturalization information from USCIS data systems to reduce the administrative burden of accessing, reporting, and sharing information and to improve connectivity between USCIS systems. The Enterprise Citizenship and Immigration Services Centralized Operational Repository serves as an intermediary database for current read-only application systems that require access to immigration and naturalization data. As an intermediary database, the Enterprise Citizenship and Immigration Services Centralized Operational Repository supports workflow management, performance measurement, and information sharing requests from external users.[17] Further, consolidating multiple data systems into one centralized repository enhances security and the management monitoring of data, and accuracy of immigration and naturalization data. The Enterprise Citizenship and Immigration Services Centralized Operational Repository is an Enterprise Data Warehouse and Operational Data Store that supports three primary functions:

- Data Retrieval – the Enterprise Citizenship and Immigration Services Centralized Operational Repository incrementally retrieves and stores an exact copy of USCIS information from connected source systems via an Extract Transform and Load (ETL)[18] process. The Extract Transform and Load functionality brings data to the Enterprise Citizenship and Immigration Services Centralized Operational Repository in accordance with an established schedule unique to each system. This allows USCIS to preserve the integrity and accuracy of the information derived from USCIS source systems.
- Data Storage – the Enterprise Citizenship and Immigration Services Centralized Operational Repository is a data repository for USCIS systems that do not have a

[16] A letterhead memorandum (LHM) is a memorandum on FBI letterhead indicating the disclosure of the content in the memorandum may be attributed to the FBI. It usually has a cover communication containing administrative data to accompany the transmittal.
[17] USCIS may share information maintained by the Enterprise Citizenship and Immigration Services Centralized Operational Repository if an external agency (e.g., Department of Justice, Department of State) has access to a system that connects with the Enterprise Citizenship and Immigration Services Centralized Operational Repository (e.g., Person Centric Query Service).
[18] Extract Transform and Load refers to a trio of processes that are performed when moving raw data from its source to a data warehouse, data mart, or relational database.

repository function of their own or systems that USCIS decommissioned and replaced with another system.

- Data Dissemination and Transaction Reporting – the Enterprise Citizenship and Immigration Services Centralized Operational Repository, when queried, sends data including transaction and reporting data about USCIS source systems to another interconnected USCIS system. The receiving system uses the data for mission-related operations, such as adjudicating a benefit, detecting fraud, or scheduling a benefit requestor's appointment.

The Enterprise Citizenship and Immigration Services Centralized Operational Repository stores the majority of CPMS data to support agency data management and reporting efforts.

***Global***[19]

Global is a source system of the Enterprise Citizenship and Immigration Services Centralized Operational Repository that provides case management functionality with a one-way connection to the Enterprise Citizenship and Immigration Services Centralized Operational Repository. Global is used to track and manage casework, schedule interviews, update relevant findings and decisions, generate reports, and assess the effectiveness of asylum pre-screening. Global provides a means for automated tracking of asylum cases as they progress from application filing through final decision of grant, denial, or referral to a U.S. Immigration Court. Global displays CPMS background check information on benefit requestors.

***Standard Management Analysis Reporting Tool (SMART), Tableau, Databricks***

Standard Management Analysis Reporting Tool (SMART) tracks and monitors the status of immigrant and nonimmigrant benefits requests and assists USCIS in the decision-making processes associated with immigration cases, case files, locations, and case metrics. The Standard Management Analysis Reporting Tool is a legacy enterprise reporting tool that supports USCIS' mission by providing accurate and useful information to USCIS users responsible for managing the integrity of immigration systems. The Standard Management Analysis Reporting Tool provides CPMS data to generate and reconcile Application Support Center reports. The Standard Management Analysis Reporting Tool is based on an Oracle tool called Oracle Business Intelligence Enterprise Edition (OBIEE). It does not store any data and is only able to display data to the end user via a report. The Standard Management Analysis Reporting Tool accesses the Enterprise Citizenship and Immigration Services Centralized Operational Repository Benefits Mart to retrieve form data from relevant case management systems to create reports for USCIS

[19] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE CITIZENSHIP AND IMMIGRATIONS SERVICES CENTRALIZED OPERATIONAL REPOSITORY (ECISCOR) (DHS/USCIS/PIA-023), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

field offices. The Enterprise Citizenship and Immigration Services Centralized Operational Repository queries information from multiple USCIS systems and creates and compiles reports pertaining to immigration benefits or cases, A-file tracking, and naturalization in one centralized location. Other enterprise tools with connections to CPMS that are used for reporting include Tableau and Databricks. These systems have database connections with CPMS and pull CPMS data on performance and other useful aggregated metrics for executive decision-making.

***Person Centric Identity Service (PCIS)[20]***

The U.S. Person Centric Identity Service is in an agency-wide effort to use enhanced business processes and emerging technologies to improve the reliability, accuracy, and completeness of identity-based biographic and biometric information across USCIS and other DHS immigration-related systems. The Person Centric Identity Service system compiles and aggregates individual applicant data[21] related to benefit requests, including CPMS biometric and background check data. This allows PCIS to present identity profiles in a single data set about an individual's identity history to support adjudicative efficiency. To improve completeness and reliability of relevant data, USCIS is leveraging existing Information Technology (IT) systems and using the Person Centric Identity Service to enhance identity management across USCIS and other DHS components that rely on immigration records to accomplish their missions. Organizing and managing identity data in a "person centric" manner requires Person Centric Identity Service to aggregate biometric data, biographic information, immigration status, and immigration history into a single identity profile. These profiles are stored in the Identity Index. This means that an individual's identity data is uniquely and accurately compiled so that each immigration benefit application, petition, or request, submitted to USCIS, each encounter with DHS[22] through administrative immigration proceedings before the U.S. Department of Justice (DOJ), [23] and any visa information collected by the U.S. Department of State (DOS),[24] is accurately associated with that individual.

The CPMS Background Check provides Person Centric Identity Service users with

[20] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE PERSON CENTRIC IDENTITY SERVICE (PCIS) (DHS/USCIS/PIA-087), *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[21] The Person Centric Identity Service obtains comprehensive person-centric data (e.g., individual's immigration history, status, and biographic and biometric identity information) and stores it in an "Identity Index" which contains Person Centric Identity Service identity data profiles established for applicants, beneficiaries, representatives, interpreters, preparers, and sponsors. The information contained therein is stored and aggregated, along with their corresponding transactional records, such as immigration benefit requests.
[22] DHS components include the U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP).
[23] The Department of Justice Executive Office for Immigration Review (EOIR) handles immigration court proceedings.
[24] The Department of State may need DHS information for purposes such as visa adjudications and consular reviews.

background check information derived from biometric and biographic data. The background check information is available to other case management systems through direct system integration with the CPMS. Results from background checks are provided from the following databases, as appropriate: FBI Response, Automated Biometric Identification System watchlist status, and FBI Name Check.

The CPMS Vetting Service provides an enhanced vetting service, utilizing Person Centric Identity Service sophisticated logic to enable the re-use of individuals' previously submitted biometrics. As such, this vetting service will increase Application Support Centers' efficiency and speed by allowing individuals to be scheduled for shorter biometrics appointments. If an individual's previously collected biometrics cannot be verified through the CPMS Vetting Service, their 10 fingerprints will be submitted again at an Application Support Center.

***ATLAS[25] (not an acronym)***

DHS and USCIS developed ATLAS to automate, streamline, and support accurate exchange of data among USCIS, DHS, and non-DHS systems used to support biometric and biographic-based screening and vetting of immigration requests. ATLAS is used as both an automated check service platform and a rule-based screening platform for USCIS.

In addition to the automated background check service, ATLAS serves as a rules-based screening tool to screen immigration requests. ATLAS screens background and security check information for enhanced data correlation and screening - highlighting areas within a case requiring additional review. This information helps USCIS to:

- Detect potential attempts to commit fraud, egregious public safety concerns, and terrorist threats earlier in the immigration benefit request process;
- Demonstrate the fidelity of the individual's biographic and biometric information; and
- Identify data discrepancies more efficiently.

When an individual files an immigration request with USCIS, biographic data from the individual's form submission is captured in a USCIS adjudicative case management system (e.g., USCIS ELIS,[26] Global). For immigration requests that require biometric-based (e.g., fingerprint) checks, USCIS stores the biometrics that have been collected at Application Support Centers, at U.S. embassies, or in the field in CPMS and creates an encounter record in the DHS Automated

[25] *SEE* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR ATLAS (DHS/USCIS/PIA-084), *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[26] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE USCIS ELECTRONIC IMMIGRATION SYSTEM (ELIS) (DHS/USCIS/PIA-056), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

Biometric Identification System[27] and the replacement system, Homeland Advanced Recognition Technology system.[28] ATLAS reads encounter data from CPMS and associates it with data from other systems to identify potential patterns of fraud or security concerns. ATLAS connects with CPMS through a read-only Application Program Interface. If a potential issue is detected, a case is created in the Fraud Detection and National Security Data System (FDNS-DS).[29]

# Privacy Impact Analysis

### Authorities and Other Requirements

The collection, use, maintenance, and dissemination of biometric and associated biographic information, including Social Security numbers are covered under the Immigration Biometric and Background Check (IBBC) System of Records;[30] 8 U.S.C. 1101 and 1103; 8 Code of Federal Regulations (CFR) 103.16(a); and 8 CFR 103.2(b)(9).

This update does not change the CPMS Authority To Operate (ATO), which was issued on October 31, 2014. CPMS is part of the Ongoing Authorization program. As such, CPMS will have an ongoing Authority To Operate 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 Paperwork Reduction Act and are accounted for under each information collection (i.e., applications and petitions) that requires its collection.

### Characterization of the Information

This update does not impact the collection of information in CPMS. USCIS continues to collect and maintain information as outlined in the "Overview" section of the original Privacy Impact Assessment. The new implementation of CPMS 2.0, the modernization of CPMS's Data Change Delete Request Form (G-1273), and the implementation of CPMS-Biometric Enrollment

---

[27] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-002 (2012) *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

[28] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART) INCREMENT 1, DHS/OBIM/PIA-004 (2020), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

[29] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICE, PRIVACY IMPACT ASSESSMENT FOR THE FRAUD DETECTION AND NATIONAL SECURITY DATA SYSTEM (FDNS-DS), DHS/USCIS/PIA-013(a) (2016), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[30] *See* DHS/USCIS-018 Immigration biometric and Background Check (IBBC) System of Records, 83 Fed. Reg. 36950 (July 31, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.

Tool, which replaced LiveScan, does not introduce a new collection of information. The new interconnections with Enterprise Citizenship and Immigration Services Centralized Operational Repository, which stores CPMS data; Standard Management Analysis Reporting Tool, which provides data to generate and reconcile reports; and Global, which provides CPMS information related to benefit requester background checks provide information to CPMS to enhance and streamline CPMS functionality.

**Uses of the Information**

The modernization of CPMS's Data Change Delete Request Form (G-1273) and the implementation of CPMS 2.0, decommissioning of LiveScan, and the new interconnections with CPMS 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) support domestic and foreign data sharing.

**Notice**

USCIS provides general notice about system changes through this Privacy Impact Assessment update and through the existing System of Records Notice (SORN) (DHS/USCIS-018 Immigration Biometric and Background Check (IBBC)). These documents provide additional transparency about USCIS biometric check, biographic background check, identity verification and resolution, card production record systems, and data sharing efforts. The Privacy Notice located on the instructions for each relevant USCIS 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 Privacy Impact Assessment 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 through interaction with USCIS personnel and Privacy Notices on forms/collection instruments. USCIS, however, does not provide explicit notice at the time of collection that the information may be stored in CPMS. Regardless of storage location, CPMS records are governed by USCIS's policies and safeguards regarding the 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 identification and benefits cards and support background check processes.

**Information Sharing**

Information sharing does not change with these updates to CMPS. USCIS shares information with the FBI to submit Name Check requests for purposes of adjudicating certain USCIS benefit requests. FBI records are searched to determine whether an individual has a record that may have an impact on the individual's eligibility for the immigration benefit requested. USCIS also initiates Name Checks for each individual who will be placed in removal proceedings prior to the issuance of the Notice to Appear. Any derogatory "hits" for individuals submitted to the FBI automatically trigger review by a specialist at the National Benefits Center (NBC) before USCIS may take any action based on the hit.

USCIS provides the Department of State Bureau of Consular Affairs read-only access to CPMS for visa and passport adjudication responsibilities, as well as fraud detection and investigation.

Asylum and refugee applicant fingerprints and limited biographic data are shared with the Department of Defense (DoD) to allow for recurrent vetting. The Memorandum of Agreement on Information Sharing and Technology Partnering Relating to Identity Verification and Screening Activities between DoD and DHS governs the use of that data. Sharing data supports the adjudication of asylum and refugee benefits requests, the assessment or refutation of claims (whether available DoD data contradicts the application or demonstrates the applicant poses a security threat), and ongoing checks where DoD or other data shows a security threat that could render an applicant ineligible for an immigration benefit or status.

Currently, USCIS submits queries for asylum and refugee claimants to limited foreign partners through OBIM's Automated Biometric Identification System, and eventually the replacement system – the Homeland Advanced Recognition Technology system. Follow-on queries requesting additional information are handled through a manual process, though also must traverse OBIM's biometric system between partners. CPMS interfaces through the OBIM biometric system with the biometric systems of Australia, New Zealand, and Canada, where a signed information sharing agreement accounting for information handling and privacy safeguards is in place. CPMS stores and sends responses to support requests for additional information from foreign partners. Special Protected Class data will continue to be filtered out, as required by statutes, regulations, and DHS policy.

**Redress**

An individual may seek access to their USCIS records by filing a Privacy Act or Freedom of Information Act (FOIA) request. Only U.S. citizens, Lawful Permanent Residents (LPRs), and covered persons from a covered country under the Judicial Redress Act (JRA) may file a Privacy Act request. Individuals not covered by the Privacy Act or Judicial Redress Act 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 a FOIA exemption. An individual may file a Privacy Act or FOIA request to view their USCIS record(s), via mail to the following address or file online at https://www.uscis.gov/records/request-records-through-the-freedom-of-information-act-or-privacy-act:

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

Some information requested may be exempt from disclosure under the Privacy Act or FOIA because information may contain law enforcement sensitive information, the release of which could possibly compromise ongoing criminal investigations. Additional information about Privacy Act and FOIA requests for USCIS records is available at http://www.uscis.gov.

**Auditing and Accountability**

USCIS ensures that practices stated in this Privacy Impact Assessment update 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 Amazon Web Services Cloud infrastructure, which is a public cloud designed to meet 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.[31] The Amazon Web Services Cloud is Federal Risk and Authorization Management Program (FedRAMP)-approved and authorized to host personally identifiable information.[32] 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 data, which are validated during the security authorization process. These technical and security controls limit access to USCIS users and mitigate privacy risks associated with unauthorized access and disclosure to non-USCIS users. Further, DHS security specifications

[31] Public clouds are owned and operated by third-party service providers whereas private clouds are those that are built exclusively for an individual enterprise.
[32] *See* https://marketplace.fedramp.gov/%23/product/aws-us-eastwest?status=Compliant&sort=productName.

also require auditing capabilities that log the activity of each user to monitor for any 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.

USCIS is responsible for all personally identifiable information 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.[33] 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. USCIS has verified through a risk assessment that the Amazon Web Services Cloud meets all DHS privacy and security policy requirements.

All USCIS users and contractors are required to complete annual privacy and computer security awareness training to ensure their understanding of proper handling and securing of personally identifiable information. The annual Privacy Training addresses appropriate privacy concerns, including Privacy Act obligations (e.g., System of Records Notices, Privacy Act Statements/Notices). The Computer Security Awareness Training examines appropriate technical, physical, and administrative control measures to safeguard information. In addition, Quality Assurance Reviewers must complete quality assurance calibration sessions. The USCIS Office of Privacy maintains certificates of training records on all users. Access to systems and data is denied if required training is not completed.

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

[33] *See* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

## Responsible Official

Angela Y. Washington
USCIS Chief Privacy Officer
U.S. Citizenship and Immigration Services
U.S. Department of Homeland Security
(202) 570-8327

## Approval Signature

MASON C CLUTTER
Digitally signed by MASON C CLUTTER
Date: 2024.05.03 15:07:50 -04'00'

Mason C. Clutter
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717