Privacy Impact Assessment

for the

Customer Profile Management System

DHS Reference No. DHS/USCIS/PIA-060(d)

September 27, 2024

Homeland
Security

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Citizenship and Immigration Services (USCIS) Customer Profile Management System (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") issued a secure card or travel document identifying the receipt of an immigration benefit. This Privacy Impact Assessment (PIA) update is to document the planned implementation of the DHS Office of Biometric Identity Management (OBIM) algorithm for biometric face verification (hereinafter referred to as "face verification" or "1:1" matching) for Form I-765, *Application for Employment Authorization* (hereafter, Form I-765), during adjudication to ensure that the photo submitted by the individual matches a previously taken photo of the individual stored within OBIM's Automated Biometric Identification System (IDENT).[1] The implementation of the biometric face verification service is being conducted to enhance the integrity of USCIS information, improve adjudications efficiency, and prevent fraud.

Overview

USCIS oversees lawful immigration to the United States and receives and adjudicates benefits requests and forms related to immigration benefits. USCIS captures biographic and biometric data from benefit requestors to facilitate the following critical 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 data duplication, including a more significant 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 implemented CPMS to centralize and improve the gathering of biometric and biographic data into a single repository to reduce the burden on USCIS employees. The overall purpose is to serve as a person-centric repository of all biometric and biographic data from benefit requestors. This system captures and maintains all biometric data in other USCIS systems and manages, as the authoritative source, the issuance of benefit cards to non-U.S. citizens; facilitates identity verification; facilitates the performance of criminal and national security background checks; and supports domestic and foreign data sharing. Its crucial functionality includes the following:

[1] *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-001 (2012 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

1. Provides the ability to collect, maintain, and locate biometric data;
2. Supports information sharing where a biometric is the primary data element; and
3. Facilitates using the information for biometric-based identity verifications and background checks.

The primary function of CPMS is to provide USCIS with the capability to store and reuse biometric images and biographic information for USCIS benefit requestors. This allows USCIS to obtain a person-centric view of interactions between an individual and USCIS.

Reason for the PIA Update

USCIS is updating this Privacy Impact Assessment to discuss the development, evaluation, and planned implementation of the OBIM algorithm for biometric face verification to ensure that the photo submitted by the individual matches with a previously government captured photograph of the individual during adjudication of Form I-765. *Application for Employment Authorization*. The initial implementation is limited to I-765 filing categories currently eligible for electronic filing; if the implementation of the algorithm for Form I-765 proves beneficial, USCIS plans to leverage this facial verification technology across all I-765 eligibility categories, regardless of the filing medium. In time, USCIS intends to expand face verification to all immigration benefit request types.

USCIS faces the challenge of processing and adjudicating more benefit requests than ever while leveraging existing resources. To expeditiously deliver on its promises of fairness, integrity, and respect for all applicants, USCIS is examining opportunities to leverage technology in processing applications, petitions, and requests. With the creation and expansion of parole processes, the increase in asylum application filings, the increase in the categories of foreign nationals eligible for Temporary Protected Status (TPS),[2] and the resumption of the family reunification parole processes, USCIS has seen an increase of over 50% in receipts of Form I-765.[3] The monthly volume of Form I-765 receipts increased from 230,162 in October 2022—when DHS created and then began expanding certain parole processes, including Uniting for Ukraine (U4U);[4] the Venezuelan parole process; and the parole processes for Cubans, Haitians, Nicaraguans, and Venezuelans (CHNV)[5]—to 348,572 in September 2023. Overall receipts for the current calendar year (2024) are projected to increase an additional 50%.

[2] For more information on Temporary Protected Status, *see* https://www.uscis.gov/humanitarian/temporary-protected-status.

[3] For more information, *see* https://www.uscis.gov/i-765.

[4] For more information on Uniting for Ukraine (U4U), *see* https://www.uscis.gov/ukraine.

[5] For more information on the Processes for Cubans, Haitians, Nicaraguans, and Venezuelans, *see* https://www.uscis.gov/CHNV.

Certain noncitizens present in the United States file Form I-765 to request employment authorization and issuance of a Form I-766, *Employment Authorization Document*. Other noncitizens whose immigration status authorizes them to work in the United States without restrictions may also use Form I-765 to apply to USCIS for an Employment Authorization Document (EAD)[6] as evidence of their employment authorization. In calendar year 2023, over 820,000 applicants electronically filed Form I-765—the initial pool of applicants selected for facial verification implementation. At a time when receipts have grown rapidly and are expected to continue doing so, USCIS has prioritized the processing of Form I-765 for several eligibility categories, including initial requests for employment authorization based upon pending asylum applications, which are required by USCIS regulations to be adjudicated within 30 days of receipt.[7] Adjudicating Form I-765 requires, in part, that USCIS verifies the identity of the individual seeking an Employment Authorization Document and obtains a photo from the individual of sufficient quality to produce an Employment Authorization Document.

Currently, the Form I-765 instructions require applicants to submit two printed identical color passport-style photographs of the applicant taken recently.[8] Some applicants for employment authorization travel to and pay a third-party company or service to take and print passport-style photos. Individuals must then send by post the hardcopy pictures to USCIS for processing. Current USCIS processes for handling such pictures require that the pictures be scanned into USCIS case management systems or physically attached to the paper Form I-765. Scanning creates and stores an electronic version of the photograph in USCIS systems that then may be printed on an Employment Authorization Document. Individuals who fall within certain Form I-765 employment eligibility categories may file their application electronically through a myUSCIS online account.[9] Individuals filing the Form I-765 electronically have the option to upload the required passport-style photographs with their application. Individuals who do not provide a photograph or provide a poor-quality photograph are scheduled to attend an in-person Application Support Center appointment to submit the required photo only.

USCIS can significantly streamline case processing by using technology to run automated background checks and automatically trigger systematic checks to determine if an individual has a relevant criminal history or may pose a national security or public safety concern.[10] One step that has not yet been fully automated is identity validation and verification for adjudication and

[6] The Form I-766 is the Employment Authorization Document. For more information, *see* https://www.uscis.gov/green-card/green-card-processes-and-procedures/employment-authorization-document.
[7] 8 CFR 208.7(a)(1).
[8] For more information and a copy of the Form I-765, please visit https://www.uscis.gov/i-765.
[9] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE MYUSCIS ACCOUNT EXPERIENCE, DHS/USCIS/PIA-071 (2017 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[10] Cases that present national security or public safety concerns or have a derogatory response to a criminal history check require manual review by an Immigration Services Officer (ISO) to resolve.

benefit card production. Below are the two ways identity validation and verification for Form I-765 currently occur.

Verification Method 1

The first method by which applicants currently have their identity verified is by a USCIS adjudications officer comparing an applicant-submitted photograph with another photograph. The Form I-765 instructions require each applicant to submit two passport-style photographs. When filing the Form I-765 electronically, a picture may be uploaded as a digital image using the USCIS online filing platform. Applicants are further required to submit photocopies of identity documents with photographs, such as passports or driver's licenses, that USCIS adjudicators use to manually compare against the passport-style photograph submitted with the benefit request to verify that the individual is the same person.

Verification Method 1 cannot be used when the photograph's scan quality is inadequate for Employment Authorization Document production. When this occurs, the applicant is required to appear for an Application Support Center appointment. In those instances, it will be necessary to verify the applicant's identity using Verification Method 2.

Verification Method 2

The second method by which applicants currently have their identity verified is by in-person human comparison. USCIS will schedule a Form I-765 applicant to appear at an Application Support Center for a biometrics services appointment. During the initial stages of the appointment, the Application Support Center personnel review the identity documents of the applicant (if any)[11] and conduct a manual identity verification prior to photo collection. In addition, if supplied, the USCIS personnel compare the biographic data from the identity document with the information on the biometrics appointment notice. Verification Method 2 is currently required for most employment eligibility categories.

Because of the time required to schedule an applicant for an in-person biometric appointment, the Verification Method 2 process for Form I-765 adjudication can take up to three weeks or longer, especially if there are delays in mailing biometric appointment notices from the Application Support Center. Lengthy processing times can also occur when large volumes of Forms I-765 require Verification Method 2 or if an applicant requests to reschedule their appointment. USCIS needs to optimize the scheduling of appointments at Application Support Centers for all applications that require the in-person collection of fingerprints for background and

[11] Certain populations of applicants are not required to have identity documents. USCIS has established procedures for individuals who attend an Application Support Center appointment without a photo ID. USCIS uses biographic matches and questions to verify identity.

security checks (not just the Form I-765), as Application Support Centers service all USCIS applications that require biometric collection.

While implementation at initial deployment will be limited to electronically filed Form I-765s and photo-only Application Support Center appointments (referred to as "Code 2" appointments), the intent is to eventually utilize biometric face verification for all Form I-765s regardless of filing method.

The biometric face verification technology will be implemented using a phased approach. Beginning with an incremental rollout for Form I-765, the implementation will start with select eligibility categories, progress to all Form I-765s, and then expand to other form types. As confidence solidifies and technology allows, more forms will utilize the facial verification service, beginning with those forms that do not require in-person biometric verification.[12] This Privacy Impact Assessment update details the testing and privacy risk mitigation measures that have been implemented in support of the Form I-765; these mitigation measures also will be relevant and apply to future expansion to other forms. USCIS will update this Privacy Impact Assessment and any other related privacy compliance documents as this initiative expands, as necessary, to ensure all privacy risks are identified, documented, and mitigated transparently.

Study of Biometric Verification

USCIS currently conducts biometric identity verification leveraging an individual's fingerprints, such as when they appear for interviews. This service is provided by OBIM and is accessed by CPMS through a system-to-system service call, with the results of the verification being available to USCIS in seconds. OBIM also operates an algorithm for biometric face matching. Identity verification using the face, referred to as face verification or 1:1 matching, is currently leveraged by several DHS Components.[13] The facial verification service performs 1:1 identity verifications using up to five previously captured photos for a particular identity to improve accuracy rates. The photos that match can be recorded as a new encounter in the Automated Biometric Identification System per the decision of the business user of the service.[14]

[12] For example, certain individuals filing Form I-131, *Application for Travel Documents,* may not be required to attend an Application Support Center appointment.

[13] U.S. Customs and Border Protection (CBP) Entry and Exit Operations are the principal production users of biometric identity verifications using face. CBP routinely leverages OBIM's face verification service.

[14] OBIM is in the process of implementing the Homeland Advanced Recognition Technology System (HART) to replace the legacy Automated Biometric Identification System as the primary DHS system for storage and processing of biometric and associated biographic information for national security; law enforcement; immigration and border management; intelligence; background investigations for national security positions and certain positions of public trust; and associated testing, training, management reporting, planning and analysis, development of new technologies, and other administrative uses. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART) INCREMENT, DHS/OBIM/PIA-004 (2020 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

For both the fingerprint and facial verification services, OBIM uses algorithms to compare the submitted biometric (called a "probe") against previously collected biometrics (called "candidates"). OBIM operates and maintains the Automated Biometric Identification System, the most extensive automated biometric identification system in the U.S. government, which stores and processes biometric data—digital fingerprints, photographs, iris scans, and facial images. The Automated Biometric Identification System is the central DHS-wide system for storage and processing of biometric and associated biographic information for national security; law enforcement; immigration and border management; intelligence; background investigations for national security positions and certain positions of public trust; and associated testing, training, management, reporting, planning and analysis, or other administrative uses. The Automated Biometric Identification System links biometrics with biographic information to establish and verify identities. The system also stores and manages identities for all previously collected biometrics from DHS Components, such as USCIS, CBP, and U.S. Immigration and Customs Enforcement (ICE), as well as Department of State (DOS), Department of Defense (DOD), and others.

Due to recent increases in Form I-765 filings, USCIS proposed using OBIM's facial verification service to conduct facial identity verification for Form I-765 adjudication and Employment Authorization Document production. USCIS believes this facial verification technology could significantly reduce case processing time and reduce human recognition bias[15] when processing Form I-765s by reducing time spent by adjudicators on paper examinations and reducing the need for applicants to appear at an Application Support Center for in-person identity verification and photo submission. USCIS first tested the technology to ensure its efficacy and accuracy for people of different ethnicity, age, and other variables.

USCIS developed a comprehensive study of the use of technology to conduct biometric face (photo) identity verification for Form I-765 applicants. Currently, these Form I-765 applicants are scheduled[16] to attend an in-person appointment at an Application Support Center to obtain a photo of sufficient quality for Employment Authorization Document production. The study was initially conducted to analyze and obtain information for cases where individuals paroled by CBP under Immigration and Nationality Act (INA) section 212(d)(5) authority later seek employment authorization from USCIS based on that parole status (referred to as the "(c)(11)" employment

[15] Face Recognition by Humans and Machines: Three Fundamental Advances from Deep Learning, Annual Review of Vision Science Volume 7, 2021 O'Toole, pp 543-570; human recognition bias may be demonstrated by own-race bias. The National Institutes of Health describes the own-race bias as "a reliable phenomenon across cultural and racial groups where unfamiliar faces from other races are usually remembered more poorly than own-race faces."

[16] Historically, USCIS has scheduled (c)(11) I-765 applicants to attend an in-person Application Support Center appointment due to having low-quality scanners that are unable to scan a high enough quality photograph effectively. At the time, given that the population was relatively small, USCIS required these individuals to attend an in-person Application Support Center appointment.

eligibility category).[17] However, a more widespread use case was soon realized; if the testing of OBIM algorithm facial matching proved successful, USCIS would then request Form I-765 applicants submit photographs and use photo identity verification to confirm applicant identity instead of scheduling applicants for in-person Application Support Center appointments. This change would verify identity, reduce unnecessary burden on the public, and increase the agency's standard for ensuring benefit integrity.

Biometric identity verification that occurred during the study, and any specific results obtained from the study, were not used for the actual adjudication or investigation of any Form I-765. The main purpose of the test was to analyze the effectiveness of the OBIM algorithm as applied to USCIS photos for potential use in the adjudication of the Form I-765.

USCIS conducted the testing to determine the accuracy and equity in False Non-Match Rate (FNMR)[18] across demographic variables such as age, gender, and race/ethnicity. While OBIM's accuracy is impressively high and the False Non-Match Rate values for face matching are low, it is important to note that these rates are impacted by photo quality. Issues of lighting, rotation, the direction a person is facing, items obscuring the photo such as a headdress or eyewear, and whether the photo's background is plain or busy can significantly impact the results of biometric matching. USCIS's goal for this test was to evaluate the impact of quality photographs for biometric identity verifications and determine a False Non-Match Rate for USCIS submissions, especially since USCIS has very high standards for photo capture due to card production objectives.

USCIS did not limit the testing to any specific Form I-765 employment eligibility categories as there would not be enough test photos to determine the efficacy of the OBIM algorithm. Calculating valid results for the algorithm test required the largest dataset possible. The dataset needed to include as many observations of key demographic variables as possible to produce valid results. If this test were limited to only photos submitted supporting specific Form I-765 employment eligibility categories, it would have been less likely to produce usable results for the areas of interest, such as race or ethnicity.

USCIS did not exclude nor identify if the photo represented an applicant in a special protected class.[19] USCIS ensured that all protections remained in place for 8 U.S.C. § 1367, and no specific information about classifications would be shared during the study. The testing phase included all Form I-765 employment eligibility categories. USCIS wanted to obtain a significant

[17] *See* 8 CFR 274a.12(c)(11) (which describes that a noncitizen paroled into the United States temporarily for urgent humanitarian reasons or significant public benefit pursuant to section 212(d)(5) of the Act is eligible for employment authorization).

[18] False Non-Match Rate refers to when the matching service incorrectly determines that two instances of the same person, as established by a trained face examiner, are different persons.

[19] Special protected classes include, but are not limited to, those individuals protected under 8 U.S.C. § 1367, INA 208, and INA 209.

data set for applicant-submitted photographs and Code 2 Application Support Center appointments to determine the False Non-Match Rates.

The following limitations were applied to the photos submitted by USCIS for the study:

- Age of photo: USCIS only included photos that were less than five years old.
- Age of applicant: the applicant's age at the time of photo submission must have been at least 12 years and nine months. Applicants under this age do not have an identity established in the Automated Biometric Identification System as they are not eligible for fingerprint capture.
- USCIS analyzed all potential photos in CPMS to identify applicants who have naturalized and are now U.S. citizens and excluded their photos from the study.

Along with the set of photos, USCIS sent the following data from CPMS to OBIM for each photo to enable later analysis of the study results:

- An encounter identification number (EID) or fingerprint identification number (FIN) for each photo
- Race/ethnicity (if available)
- Age
- Gender
- Country of Birth (if available)
- Country of Residence (if available)
- Collection Type (mailed, uploaded, or captured at an Application Support Center)
- Form Type (I-765 only)

USCIS submitted a set of approximately 341,000 photos associated with Form I-765 applicants ("probe photos") to OBIM using a secure file transfer for this test. OBIM then leveraged the 1:1 identity verification against as many as five photos ("candidate photos") for that same identity in the Automated Biometric Identification System. USCIS utilized OBIM's defined thresholds for matching, and OBIM returned the results of the biometric matching to USCIS via secure file transfer. For each photo submitted, OBIM provided results as: "match," "no match," and in instances where the identity did not exist in the Automated Biometric Identification System database, "not found." Analysts then examined the results of the test to calculate overall accuracy rates and the False Non-Match Rate, as well as specific demographics (where sample sizes allowed), variables such as age, gender, race, ethnicity (if asked), and country of birth.

USCIS completed the initial testing phase using only Form I-765 applications. This testing phase was limited to photos that were previously submitted by customers (scanned or uploaded) in association with a Form I-765 or captured at an Application Support Center photo-only appointment (referred to as a "Code 2" appointment) in support of a Form I-765. Per USCIS rules for enrollment, testing used only photos that were not previously stored in OBIM's Automated Biometric Identification System database, to eliminate the possibility that the test would ask the facial verification service to compare the photo to itself. USCIS also could ensure these photos were not enrolled in the Automated Biometric Identification System because Application Support Center Code 2 appointments and scanned passport photos are not currently enrolled in the Automated Biometric Identification System and are not used for criminal history checks. Application Support Center Code 2 appointment photographs are used only for benefit card production.

Upon completion of the testing, the results proved favorable and aided in the decision to move forward with facial verification to support automated Form I-765 processing. The testing revealed the True Match Rate (TMR) supported automated operations. True Match Rate is the rate at which the facial verification algorithm correctly matches two instances of the same person. USCIS determined that an internal review to confirm the True Match Rate produced by the study was unnecessary because DHS's Science and Technology Directorate (S&T) also conducted testing of the OBIM facial verification algorithm. S&T independently performed nearly 10,000 photo comparisons for USCIS use cases using the facial verification algorithm for 1:1 matching and determined the facial verification algorithm to be 100% accurate for True Match Rate.

OBIM also recorded and reviewed all "no match" results, which were further categorized as either True Non-Matches[20] or False Non-Matches.[21] Trained human examiners reviewed all "no matches, " which totaled 438. According to the testing results from OBIM, the facial verification algorithm returned only a small number of False Non-Matches. Upon manual examination of the False Non-Matches identified by the OBIM testing, the vast majority of the False Non-Matches were determined to be the result of photo capture issues (e.g., poor photo quality, high-angle subject pose, aging from a juvenile to an adult between encounters, multiple faces in the candidate photo, or the subject's face being obscured). Of note, many of the photo capture issues revealed by the testing involved the photographs that were already in the Automated Biometric Identification System and not necessarily USCIS-submitted photos,[22] which have much higher

[20] True Non-Matches: Instances where—upon review and confirmation by a trained face examiner—the face verification algorithm correctly determined that the person in the probe photo was not the same person as in the candidate photo(s).

[21] False Non-Matches: Instances where—upon review and confirmation by a trained face examiner—the face verification algorithm incorrectly determined that the person in the probe photo was not the same person as in the candidate photo(s).

[22] USCIS-submitted photos refer to photos obtained in support of an application either at an Application Support

capture standards because of the need to produce secure identity documents and Employment Authorization Documents. These issues may be mitigated by improving processes at the time of photo capture—particularly in agencies without card production requirements.

The testing also uncovered approximately 400 True Non-Matches. These highlighted the administrative identity issues and errors that can be mitigated by leveraging the face verification technology. Some cases appeared to be honest mistakes where the face images of spouses and their names were mixed up. Others were administrative errors, such as associating an identity with an incorrect A-number, thereby comparing the "probe" photograph to an incorrect identity. Additionally, it is possible that some True Non-Matches were the result of fraud.

The testing results produced no discernable trends indicating potential biases or potential disparate treatment of particular populations or categories of individuals with whom USCIS typically interacts for immigration purposes. USCIS determined this by using an individual's country of birth as a proxy for skin tone, race, and ethnicity. USCIS and OBIM also manually reviewed the non-match photographs and determined only 38 out of the 438 "no matches"[23] were False Non-Matches. Of the 38, there was no discernable trend except for the photo capture issues mentioned above. To improve the customer experience and mitigate against any possible disparate treatment, USCIS has opted to develop a manual resolution queue within CPMS, through which all non-matches will be contextually reviewed by a USCIS employee trained in face examination.

For this test, the results were not stored in the Automated Biometric Identification System but were stored in CPMS, which was consistent with the appropriate retention schedule for the system. USCIS currently stores all photos obtained to support benefit requests in either of the applicable benefit's case management system, CPMS, or both. The previously captured photographs used to match against predominantly came from CBP inspection encounters; however, some DOS visa photographs may have been included. Through this verification, the Automated Biometric Identification System automatically compared the photo from each new individual to (up to as available) five best-quality photos associated with the identity in the system. OBIM currently sees a True Match Rate and False Non-Match Rate for biometric identity verifications using the face biometric comparable to established fingerprint matching metrics. Upon implementation of the facial verification service in a production environment, USCIS may choose to enroll successful matches in the Automated Biometric Identification System because enrollment will subscribe the identity to fingerprint updates that are published in the Automated Biometric Identification System, which could help the agency with identity management.

Leveraging OBIM's face verification service will provide USCIS with an additional tool to combat fraud and improve the overall accuracy of USCIS records. Because all non-matched

Center, manually uploaded electronically by the applicant, or physically mailed into USCIS (i.e., passport-style photos).

[23] 400 were found to be True Non-Matches.

photos will be manually reviewed before adjudication, administrative errors or potential fraud will be more likely to be identified and handled before issues are shared across DHS systems. This is beneficial because issues are more difficult to correct once other systems ingest the inaccurate data. USCIS will have high assurance that a True Match for a photo taken at an Application Support Center or submitted by the applicant accurately verifies that the photo relates to the actual applicant for the benefit. Based on the study results, the use of OBIM's algorithm will provide a more efficient identity verification process compared to USCIS' reliance on a human comparative analysis for identity verification. USCIS believes that OBIM's facial verification service has the potential to improve dramatically USCIS's efficiency to better serve its customers.

Implementation of the Facial Verification Service

Given the success of the testing, USCIS plans to use customer-submitted photographs uploaded as part of an electronic submission of Form I-765 through a USCIS online account instead of requesting that applicants attend an in-person Application Support Center appointment. This will reduce the burden on the public while still upholding benefit integrity. USCIS plans to leverage this technology in the future across a broader array of forms.

The established processes for individuals to submit photos required for their application will not change or be affected by the implementation of OBIM's facial verification service. Implementation at deployment will initially be limited to electronically filed Form I-765s and photo-only Application Support Centers appointments ("Code 2" appointments). In time, facial verification will be employed for all Form I-765s regardless of filing method. The implementation of the facial verification service for all Form I-765s will be done as an incremental process to ensure that all technical requirements are in place, provide USCIS with opportunities to ensure the effectiveness of the facial verification service, and ensure all potential privacy and civil rights and civil liberties risks are assessed and mitigated with each phase of deployment.

Once an individual submits their photograph using an established intake channel, the photo is accepted by USCIS and added, along with the other Form I-765 information, into the appropriate USCIS case management system. Submitted Form I-765s are currently stored in two case management systems, the USCIS Electronic Immigration System (USCIS ELIS or ELIS)[24] and the Computer Linked Application Information Management System 3 (CLAIMS 3).[25] Once the case management systems ingest an applicant's photograph, they then send it to CPMS, the

[24] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE U.S. CITIZENSHIP AND IMMIGRATION SERVICES ELECTRONIC IMMIGRATION SYSTEM (USCIS ELIS), DHS/USCIS/PIA-056 (2018 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[25] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE COMPUTER LINKED APPLICATION INFORMATION MANAGEMENT SYSTEM AND ASSOCIATED SYSTEMS (CLAIMS 3), DHS/USCIS/PIA-003 (2020 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

centralized repository of biometric images used for USCIS benefit card and document production. Once the photo is stored in CPMS, it becomes immediately available for the case management systems to use in existing adjudication and card production workflows.

If an application is processed in the USCIS Electronic Immigration System, the photograph will be run through the USCIS ELIS Photo Validation Tool to help ensure the photograph is of card production quality. The USCIS ELIS Photo Validation Tool provides an automated evaluation against USCIS card photo specifications requirements. The validation requirements for the human subject of each photo are: 1) head and face are present, 2) eyes are open and visible, 3) mouth is closed, 4) subject is in front of a plain white background, 5) no red eye effect is present, 6) even lighting and contrast throughout, 7) glasses have been removed, 8) front-facing pose is presented, 9) head is not tilted, 10) the height of the head takes up at least 50% of the frame height, 11) face is centered in the frame, 12) non-religious head coverings have been removed, 13) photo has a 1:1 aspect ratio, and 14) the entire photo layout is oriented correctly. If the photo is of insufficient quality or from an individual who cannot meet the photo quality criteria,[26] USCIS will follow standard card production failure reviews and procedures to obtain an appropriate photo.

Once the photo passes the USCIS ELIS Photo Validation Tool checks, the photo is sent through an Application Programming Interface (API) to CPMS. Upon ingesting the photograph into CPMS, CPMS will vet the biographic information and metadata to determine if the photo is eligible for face verification. To be eligible for face verification, the applicant must be at least 12 years and nine months old, the photo must be associated with the correct form type and eligibility category, and an identifier (e.g., A-number) must be associated with the photo. If these criteria are not met, CPMS will respond to the USCIS Electronic Immigration System through an Application Programming Interface with a notification that the photo is "ineligible" for face verification, and OBIM's face verification algorithm will not process the photo. The photo will be retained as an encounter[27] in CPMS in accordance with the applicable retention schedule established by the National Archives and Records Administration (NARA).

If the photo passes CPMS' initial vetting, then CPMS will "call" (i.e., directly reach out) to the Automated Biometric Identification System facial verification service through an Application Programming Interface, using the applicant's A-number to see if there are any photographs housed in the Automated Biometric Identification System for that identity, or if there are multiple identities associated with the identifier.[28] No additional information is used beyond

[26] Individuals may fail to meet the photo quality criteria due to a physical characteristic that prevents them from passing the automated checks, such as religious headwear, facial paralysis, or missing an eye. These photos will be manually reviewed by USCIS personnel for decision-making. This is the same manual review process that already currently exists today for mailed-in photos.

[27] Encounter describes any event during which biometric collection occurs (e.g., photograph, fingerprints, or both).

[28] CPMS may make up to two calls to the Automated Biometric Identification System to determine if an identity exists and if the photo matches the identity.

the A-number during CPMS' initial call to the Automated Biometric Identification System. If photographs of that individual do not exist, the facial verification service will return a response of "not found." CPMS will then send a message indicating no identity was found for the subject via Application Programming Interface for the USCIS case management systems to ingest. USCIS adjudicative directorates will then follow their internal procedures to process the case. CPMS then makes a second "call" to the Automated Biometric Identification System and provides the photo so the photo can be retained as an encounter in both the Automated Biometric Identification System and in CPMS.

If multiple identities exist in the Automated Biometric Identification System, an error message will be returned to CPMS. CPMS treats this error as "ineligible" and relays the "ineligible" response to the case management systems for ingest. OBIM's face verification algorithm will not process the photo, but the photo will be retained as an encounter in CPMS.

If a single identity exists within the Automated Biometric Identification System for the identifier provided, a response is sent to CPMS indicating "identity exists." CPMS will then make a second call to the Automated Biometric Identification System, providing the photo so that face verification can be performed. Upon completion of the face verification process, the Automated Biometric Identification System will return a response of "match" or "no match." This information will be stored in CPMS associated with the encounter and posted for consumption by the appropriate case management system(s).

If the USCIS Electronic Immigration System receives a "no match" response from CPMS, the I-765 case processing will automatically pause for manual review of the applicant's photograph by a trained identity specialist. The Computer Linked Application Information Management System 3 currently does not have the technological capabilities to ingest CPMS' response. However, regardless of the case management system, a trained identity specialist will manually review any non-matched photograph submitted to the facial verification service. USCIS employees adjudicating applications in the Computer Linked Application Information Management System 3 will follow their internal procedures to review the identity information found and displayed in CPMS.

All photographs returned as a "no match" from the Automated Biometric Identification System are automatically placed into a manual review queue within CPMS. These photographs, and contextual information will be reviewed by USCIS identity specialists to determine if the photograph is a True Non-Match or a False Non-Match. If determined to be a False Non-Match, the employee will indicate as such. CPMS will then broadcast a "match" message to the case management systems. If the case is processed in the USCIS Electronic Immigration System, the pause will be terminated, and case processing will continue. The results indicating a successful match will be displayed in CPMS, and the photo will be available for future reuse.

If a USCIS employee determines the photograph is a True Non-Match, they will indicate it as such. CPMS will then broadcast a "no-match" message to the case management systems. The non-matched photo will be flagged in CPMS as unavailable for reuse. It will be up to the adjudicative directorate to determine what follow-up action—if any—is required. This process does not impact the current intake processes for photograph submission and will only be a backend change to internal USCIS processes. Further, existing photo quality or identity verification processes, such as requesting a new photo or requiring the individual to have their photo taken at an Application Support Center, will remain unchanged.

If OBIM'S facial verification service is used to verify a photograph that is later rejected by the USCIS card production facility for insufficient card production quality, USCIS employees will attempt to re-size, re-crop, or adjust the contrast to enhance the photograph to meet sufficient quality standards. This task is performed by leveraging tools in the case management systems. If these efforts fail, the adjudicating officer may need to take remedial action, such as scheduling the applicant for an Application Support Center appointment or requesting additional evidence to obtain additional card production quality photographs. The case management system will communicate this to CPMS, and the photo of insufficient quality will be flagged to prevent future reuse.

The manual Non-Match review queue will be staffed by USCIS identity specialists, provided by the USCIS Identity and Information Management Division (IIMD), trained in facial examinations. USCIS employees will review information about the applicant, including application information, previous biometric encounters, previous photographs, and data in USCIS systems, to help determine if the photograph is a True Non-Match or a False Non-Match. If it is a False Non-Match, the trained identity specialist will indicate which photograph or contextual information (e.g., significant age gap in photos, visible body modifications, gender reassignment) led to their decision. CPMS will display a photograph line-up of up to ten of the most recent prior encounters housed in the Automated Biometric Identification System, and the trained identity specialist will select the photo(s) that the employee used to conclude that the case was a False Non-Match. Upon contextual review by the trained identity specialists and once a determination is made that the photograph is a False Non-Match, CPMS will again broadcast the results for case management systems to ingest.

The manual Non-Match review queue will also provide reportable information regarding any reasons for the no-match (e.g., an A-number mismatch). This manual resolution queue also serves to enhance the data integrity of USCIS systems and mitigate any disparate treatment on any population. Manual review will occur prior to scheduling an applicant for an Application Support Center appointment. Once implemented, the facial matching and manual resolution queue results may be used for the adjudication or investigation of Form I-765 benefits, should fraud be suspected.

Currently, only photographs submitted at an Application Support Center may be reused for future benefit applications. Photo reuse is a process by which prior USCIS-captured photographs or biometrically verified photographs submitted in support of a USCIS application are eligible to be used on future/subsequent cards, as dictated by the USCIS Policy Manual.[29] In contrast, applicant-submitted photographs may currently only be used once for the specific benefit request filed with USCIS and are not allowed to be reused for future benefit requests. Pending any required updates to USCIS policies and procedures, all photographs that are deemed a match through OBIM's facial verification service will be eligible for reuse, whether provided by the applicant at the Application Support Center or uploaded as an electronic attachment to a benefit request submitted through USCIS online account. All photographs deemed a "no match" will be flagged and unavailable for photograph reuse. After a successful face verification, OBIM will append the face-only encounter to the Fingerprint Identification Number (FIN) in the Automated Biometric Identification System as a part of the matched identity. Photos that are verified through OBIM's facial verification service will be marked available for reuse within the Automated Biometric Identification System, and those that are True Non-Matches will be flagged as non-reusable.

Once implemented, facial verification may be used to support adjudication by helping to ensure the benefit requested is given to the biometrically verified individual eligible for the benefit. Facial verification may also reduce the risk of fraud or identity theft by identifying instances of imposters and other bad actors due to the failure to verify the identity biometrically. The initial use case for OBIM's facial verification service will be electronically filed Form I-765s, intending to expand incrementally to all Form I-765 categories, regardless of submission method (i.e., electronic or paper). Facial verification may be leveraged across all form types in the future.

Privacy Impact Analysis

Authorities and Other Requirements

The collection, use, maintenance, and dissemination of biometric and associated biographic information are authorized by 8 U.S.C. §§ 1101 and 1103; 8 CFR 103.16(a); and 8 CFR 103.2(b)(9). Section 103 of the Immigration and Nationality Act (INA) provides the legal authority for the administration and adjudication of immigration and nonimmigration benefits.[30] In particular, under section 103(a)(3) of the Immigration and Nationality Act, 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 Immigration and Nationality Act. The

[29] The U.S. Citizenship and Immigration Services Policy Manual is the agency's centralized online repository for USCIS' immigration policies. The USCIS Policy Manual will ultimately replace the Adjudicator's Field Manual (AFM), the USCIS Immigration Policy Memoranda site, and other policy repositories. The USCIS Policy Manual can be found at: https://www.uscis.gov/policy-manual.

[30] 8 U.S.C. § 1103(a).

Immigration Biometric and Background Check (IBBC) System of Records Notice (SORN)[31] covers USCIS' collection, use, and maintenance of biometric information.

This update does not change CPMS' Authority to Operate (ATO), 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 Ongoing Authorization requires CPMS to be reviewed monthly and to maintain its security and privacy posture in order to retain its Authority to Operate. 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.

Characterization of the Information

This update does not alter the collection of information in CPMS. USCIS continues to collect and maintain information as outlined in the "Overview" section of this Privacy Impact Assessment and Section 2.0 of the previously published CPMS Privacy Impact Assessments[32] published on the DHS Privacy website. Implementing OBIM's facial matching algorithm for use with Form I-765 applicants does not introduce a new collection of information. USCIS has long collected photographs as part of the immigration benefit request process to enable USCIS to verify a benefit requestor's identity, conduct background checks, and produce applicable benefit cards or secure documents. With the implementation of the facial matching algorithm, the identity verification will be completed through the matching algorithm and a manual review queue, rather than the previous method by which an applicant's identity was verified by a human comparison of two photos. USCIS believes that this will provide a more accurate identity verification process. The study and ultimate implementation of the biometric face verification service is being conducted to enhance the integrity of USCIS information, improve adjudication efficiency, and prevent fraud.

Uses of the 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.

[31] *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.

[32] *See* U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services, Privacy Impact Assessment for the Customer Profile Management system (CPMS), DHS/USCIS/PIA-060 (2015 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

USCIS completed the study of OBIM's facial matching algorithm to determine the efficacy of the process and identify whether there are any populations or demographic trends illustrated in the test results that may indicate any potential biases or disparate treatment of particular populations or categories of individuals who USCIS typically interacts with for immigration purposes. During the study, USCIS used a significant data set for applicant-submitted photographs and Code 2 Application Support Center appointments to determine the possible False Non-Match Rate. The test included all Form I-765 employment eligibility categories—the intended application of OBIM's algorithm.

The test results demonstrated a high accuracy rate across the measured variables: True Match, True Non-Match, or False Non-Match. The accuracy rate was agnostic to submission type. Furthermore, results showed no discernable trends indicating potential biases or disparate treatment of particular populations or categories of individuals with whom USCIS typically interacts for immigration purposes. These testing results led to USCIS' decision to employ OBIM's face verification service.

While the volume of False Non-Matches was low, USCIS has opted to implement a secondary human review for all photos resulting in a "no match" after being run through the face verification algorithm. This was implemented to reduce potential customer burden, improve the reliability of USCIS information, and identify potential fraud. Likewise, controls will be implemented to prevent future photo reuse for all photos deemed a Non-Match by both the algorithm and the human reviewer. Photographs that are matched by the algorithm or determined to be a False Non-Match upon human review will be authorized for future reuse.

Leveraging the face verification service does not require a new collection of information by USCIS, and there is no fee charged for using the service. Once implemented, facial verification may be used to support adjudication by ensuring the requested benefit is given to the biometrically verified individual who is eligible for the benefit.

<u>Privacy Risk</u>: There is a risk that the use of the facial matching algorithm could lead to disparate outcomes for individuals.

<u>Mitigation</u>: This risk is mitigated. USCIS conducted extensive testing of the facial verification technology with OBIM to ensure its efficacy and accuracy for people of different ethnicities and ages, as well as across demographic variables such as gender and race/ethnicity. USCIS believes this facial matching technology could significantly reduce case processing time and human recognition bias when processing Form I-765s by reducing time spent by adjudicators on paper examinations and reducing the need for applicants to appear at an Application Support Center for in-person identity verification and photo submission. USCIS ensured that the study was designed to sufficiently test the impact of the algorithm on the rates of False Non-Matches in relation to country of origin, gender, skin color, and items obscuring the face, such as headdress or eyewear. The test results did not produce any trends indicating potential biases or potential disparate treatment of particular populations or categories of individuals whom USCIS typically interacts with for immigration purposes. USCIS determined this by using an individual's country of birth as a proxy for skin tone, race, and ethnicity. USCIS and OBIM also manually reviewed the non-match photographs and determined that only 38 of the test samples were returned as False Non-Matches.

Of the 38, there was no discernable trend except for the photo capture issues discussed above (e.g., poor photo quality, high-angle subject pose, aging from a juvenile to an adult between encounters, multiple faces in the candidate photo, or the subject's face being obscured). To improve the customer experience and further mitigate any possible disparate treatment, USCIS has opted to develop a manual resolution queue within CPMS, for which all "no matches" will be contextually reviewed by a trained human identity specialist.

Privacy Risk: There is a risk that information provided to OBIM as a part of the initial study may be used for unauthorized purposes outside of the original study's purpose.

Mitigation: This risk is mitigated. The test results were not retained in the Automated Biometric Identification System. USCIS and OBIM worked closely to design the study to be outside of the usual process for the facial verification matching regularly performed by OBIM.

A segregated channel was created to ensure the information used for the study remained separate from other information, instead of using the typical data transmission process in which data is automatically sent to OBIM over the existing channel and fingerprints and photographs are enrolled in the Automated Biometric Identification System. OBIM developed scripts so photos could be run against the algorithm but would not be enrolled in the Automated Biometric Identification System as new encounters. OBIM only stored the USCIS photos and related information, and all match results in a temporary file location. Once the matching and analysis occurred and the study was concluded, OBIM deleted all the records they received from USCIS.

Upon implementing the facial verification service in a production environment, USCIS may choose to enroll successful matches in the Automated Biometric Identification System because it will subscribe to the identity to fingerprint updates that are published in the Automated Biometric Identification System, which could help the agency with identity management.

Privacy Risk: There is a risk that information may be used outside of the original purpose of collection.

Mitigation: This risk is mitigated. All records are protected from unauthorized access and use through appropriate administrative, physical, and technical safeguards that include restricting access to authorized personnel who have a need-to-know. USCIS limits access to personally identifiable information by employing role-based access to backend systems to ensure access is only granted to those USCIS personnel with a need-to-know. To ensure the information is used consistently for the purposes of the original collection, USCIS administrators monitor internal and external user logs to ensure users are only accessing information related to their job functions. All USCIS personnel are thoroughly trained regarding the use of the underlying system databases and the sensitivity of the information maintained by USCIS. Additionally, all USCIS personnel are required to take the annual security and privacy awareness training.

Privacy Risk: There is a risk that the incorporation of facial verification technology into the established USCIS processes could delay or prevent issuance of an Employment Authorization Document.

Mitigation: This risk is mitigated. Through this process, USCIS collects the photo directly from the benefit requestor so that the most current and accurate photo of the benefit requestor should be available to USCIS. Benefit requestors receive prior notice through USCIS forms and form instructions about the requirement to submit photographs when filing (whether electronically or on paper) and specific standards for the photos submitted. Prior to submitting the photo or any other Form I-765 information to USCIS, benefit requestors are directed to review the photo and information to confirm it is correct. USCIS has also implemented the USCIS ELIS Photo Validation Tool to streamline this process, ensuring, to the greatest extent, that the photo collected by USCIS and run through the facial matching algorithm will likely match.

Further, Benefit requestors who cannot meet the photo quality criteria may still submit the photo to USCIS despite failing validation standards in the event the benefit requestor believes the quality issue may not be related to a photo capture error but is related to a physical characteristic such as facial paralysis, missing an eye, or other irregularity of the face that might prevent them from passing the automated checks but would pass adjudicator review of the photo.

All photographs returned as a "no match" from the Automated Biometric Identification System will automatically be placed into a manual review queue within CPMS. Photos that fail the facial matching algorithm, along with contextual information, will then be manually reviewed by a USCIS identity specialist as needed to determine if the photograph is a True Non-Match or a False Non-Match and for decision-making. This is the same manual review process that currently exists today for mailed-in photos. If the photo is found to be of insufficient quality, USCIS will follow standard card production failure reviews and procedures to obtain an appropriate photo.

USCIS also gives individuals opportunities during and after the submission of the immigration benefit request to correct information they have provided or received. If information is incorrect or could lead to a denial of the immigration benefit, USCIS will notify the benefit requester through the issuance of a Request for Evidence (RFE), a Notice of Intent to Deny (NOID), through an interview, or similar processes whereby the benefit requestor would have an opportunity to review and respond. If USCIS errs on an immigration benefit document, the benefit requestor may request that USCIS correct the mistake.

Notice

USCIS provides general notice about the system changes through this Privacy Impact Assessment update and through the existing System of Records Notice: DHS/USCIS-018 Immigration Biometric and Background Check (IBBC), which provides additional transparency about the collection and use of personally identifiable information to conduct the biometric check, biographic background check, identity verification and resolution, card production record systems, and data sharing efforts. Privacy Notices contained in the instructions for each USCIS form provide notice to individuals of USCIS's authority to collect information, the purposes of the collection, routine uses of the information, and the consequences of declining to provide the information to USCIS. Therefore, through the application process, USCIS provides individuals with 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 other processes.

The public receives notice, through USCIS forms and form instructions, about the requirement to submit photographs when filing (whether electronically or on paper) certain immigration benefit requests (e.g., Form I-765s). While USCIS forms are in English, USCIS provides translations for many public communications and alerts posted on the USCIS.gov website to increase customer accessibility to relevant immigration content. USCIS also has information about photo requirements and submission in the USCIS Policy Manual, and regularly publishes updates and alerts to the USCIS Policy Manual when needed. USCIS also updates the USCIS.gov web pages for specific processes or programs to notify benefit requestors when photos can be reused or when individuals must appear at an Application Support Center. There are certain form types where benefit requestors are not required to submit photographs with their filings but must still appear at an Application Support Center to provide their signature and allow USCIS to capture their photo to produce a proof of benefit such as an Employment Authorization Document or a Permanent Resident Card.

USCIS also provides notice of photograph submission requirements, USCIS storage and use of photographs for identity verification, and the use of OBIM's Automated Biometric Identification System for biometric identity checks via published privacy compliance documentation (see below) available on the DHS Privacy website.

- DHS/USCIS/PIA-056 USCIS Electronic Immigration System (USCIS ELIS or ELIS)[33] provides information to the public about how benefit requests are processed; the potential need for biometrics to be submitted; the transmission of information from USCIS

[33] *See* U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services, Privacy Impact Assessment for the USCIS Electronic Immigration System (USCIS ELIS), DHS/USCIS/PIA-056 (2018 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

Electronic Immigration System—including ten-print, photo, and biographic information—to the Automated Biometric Identification System for Biometric Identity Checks; and how photographs may be used for post-adjudication processing, as applicable.

- DHS/USCIS/PIA-063 Benefit Decisions and Output Processes[34] discusses the collection, verification, and use of biometrics in the production of various secure identity documents to formalize the decision and provide the benefit recipient with official documentation establishing proof of benefit.

- DHS/OBIM/PIA-001 Automated Biometric Identification System (IDENT)[35] provides notice to the public about the central DHS-wide system for storage and processing of biometric and associated biographic information for national security; law enforcement; immigration and border management; intelligence; background investigations for national security positions and certain positions of public trust; and associated testing, training, management reporting, planning and analysis, or other administrative uses.

- DHS/OBIM/PIA-004 Homeland Advanced Recognition Technology System (HART)[36] Increment 1 provides notice to the public of the intended replacement for the legacy Automated Biometric Identification System as the primary DHS system for storage and processing of biometric and associated biographic information for national security; law enforcement; immigration and border management; intelligence; background investigations for national security positions and certain positions of public trust; and associated testing, training, management reporting, planning and analysis, development of new technologies, and other administrative uses.

- DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records Notice[37] provides notice to the public about USCIS' collection, use, and maintenance of biometric information. The System of Records Notice details that the purpose of the system of records is to assist USCIS with determining an individual's eligibility for an immigration benefit request or other USCIS requests. Further, notice is

[34] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE BENEFIT DECISIONS AND OUTPUT PROCESSES, DHS/USCIS/PIA-063 (2016), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[35] *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-001 (2012 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

[36] *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 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

[37] *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.

provided that USCIS captures biographic and biometric data from applicants, petitioners, sponsors, beneficiaries, or other individuals to facilitate three key operational functions: (1) enroll, verify, and manage an individual's identity; (2) conduct criminal and national security background checks; and (3) produce benefit cards and documents as a proof of benefit.

Privacy Risk: There is a privacy risk that individuals providing information to USCIS for Form I-765 do not receive sufficient notice explaining that their information is being sent to OBIM for processing through the algorithm for biometric face verification and their photo may be retained in the Automated Biometric Identification System.

Mitigation: This risk is mitigated. This Privacy Impact Assessment update serves as notice to the public regarding the implementation of the OBIM facial matching algorithm for use during the adjudication of Form I-765. The Privacy Notice located on the instructions for each USCIS form notifies individuals of USCIS' authority to collect information, the purposes of the collection, routine uses of the information, and the consequences of declining to provide the information to USCIS. The public also receives notice through USCIS forms and form instructions about the requirement to submit photographs when filing (whether electronically or on paper) certain immigration benefit requests. USCIS also regularly updates the USCIS.gov web pages for specific processes or programs to notify benefit requestors when photos can be reused or when individuals must appear at an Application Support Center. Therefore, individuals are provided notice of the use of the information for adjudication purposes, including background investigations and identity verification, prior to and throughout the application process.

Data Retention by the Project

This update does not change the retention of information in CPMS. The electronic records in CPMS will continue to be retained for 100 years from the individual's date of birth and then destroyed in accordance with the NARA Disposition Authority Number DAA-0563-2013-0001-0005, barring any legal or other holds on the record. The information is collected to support the creation and issuance of benefit cards and the background check processes. Certain photographs submitted to USCIS with a paper filing may be retained in the physical A-File for investigative purposes or in cases that involving fraud or willful misrepresentations. A-Files have permanent value because they document enduring legal rights and have high potential research value. DHS transfers A-Files to the custody of NARA for retention for 100 years after the individual's date of birth.

Upon implementing the facial verification service in a production environment, USCIS may choose to enroll successful matches in the Automated Biometric Identification System because doing so will subscribe the identity to fingerprint updates that are published in the Automated Biometric Identification System, which could help the agency with identity management. USCIS regularly searches and enrolls data in the Automated Biometric Identification System to establish and verify the identities of individuals requesting and being adjudicated for immigration benefits, including asylum and refugee status. Enrollment of successful matches in the Automated Biometric Identification System would follow existing USCIS processes and ensure complete USCIS data is available within the system.[38] NARA approved the records retention schedule for the Automated Biometric Identification System. The records schedule requires OBIM to maintain Automated Biometric Identification System records in its custody for the various retention periods outlined in the Biometric with Limited Biographic Schedule[39] (DAA-0563-2013-0001).

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

Mitigation: This risk is partially mitigated. Although there is always an inherent risk in retaining information for any length of time, 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, they may continue interacting with USCIS throughout their life. The CPMS System Administrator is responsible for reviewing, deleting, or archiving information in accordance with the NARA-approved or DHS-approved records retention schedule. Also, security controls are in place to ensure that information is protected during this time.

Current records schedules require OBIM to maintain Automated Biometric Identification System records in its custody for the various retention periods outlined in the Biometric with Limited Biographic Schedule (DAA-0563-2013-0001). The variable retention period is necessary to support the holding of biometrics of subjects of interest in immigration and border management or law enforcement activities.

Information Sharing

This update does not modify external information sharing detailed in the previously published CPMS Privacy Impact Assessments. Within DHS, USCIS currently conducts biometric identity verifications leveraging an individual's fingerprints, such as when they appear for an interview or naturalization ceremony. This service is provided by OBIM and is accessed by CPMS through a system-to-system service call, with the results of the verification being available to

[38] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE IMMIGRATION BENEFITS BACKGROUND CHECK SYSTEMS (IBBCS), DHS/USCIS/PIA-033 (2010), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[39] *See* Biometric with Limited Biographic Schedule, *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2013-0001_sf115.pdf.

USCIS in seconds. The new implementation of the OBIM facial matching algorithm for use during the adjudication of Form I-765s expands the current information sharing activities with OBIM.

With this implementation of the OBIM facial matching algorithm during the adjudication of Form I-765s, USCIS will also use the OBIM algorithm for facial verification. OBIM's facial matching algorithm performs 1:1 identity verifications using up to five previously captured photos for a particular identity to improve accuracy rates. The verifications that match can be recorded as a new encounter in the Automated Biometric Identification System per the decision of the business user of the service.

The previously collected photographs for a given identity housed within OBIM serve as the "candidate" photographs to which the OBIM algorithm compares the applicant-submitted photograph, also called the probe photograph. Once the facial verification is performed, an encounter will be created and added to CPMS and the Automated Biometric Identification System. Once added to the Automated Biometric Identification System, an Encounter Identification Number will be added, the reason for the encounter creation and the identifier used to perform the facial verification (e.g., A-number). This is the same process used for all USCIS encounters. Automated Biometric Identification System and CPMS customers will be able to see this encounter, which is consistent with other USCIS encounters.

Privacy Risk: There is a privacy risk that data will be disclosed for purposes other than the original stated purpose and use for the information collection.

Mitigation: This privacy risk is mitigated. DHS has established policies and procedures that enable information sharing among DHS Components when there is a mission need for the information. USCIS and OBIM employ technical and security controls to preserve the data's confidentiality, integrity, and availability, which are validated during the security authorization process. These technical and security controls limit access to USCIS and OBIM users and mitigate privacy risks associated with unauthorized access and disclosure to unauthorized users.

Upon implementing the facial verification service, USCIS may choose to enroll successful matches in the Automated Biometric Identification System because doing so will subscribe the identity to fingerprint updates published in the Automated Biometric Identification System, which could help the agency with identity management. USCIS regularly searches and enrolls data in the Automated Biometric Identification System to establish and verify the identities of individuals applying for immigration benefits, including asylum and refugee status, and to assist USCIS in adjudicating benefit requests. Enrollment of successful matches in the Automated Biometric

Identification System would follow existing USCIS processes and ensure complete USCIS data is available within the system.[40]

Further, OBIM employs technical and security controls to preserve the data's confidentiality, integrity, and availability, which are validated during the security authorization process. These technical and security controls limit access to OBIM users and mitigate privacy risks associated with unauthorized access and disclosure to non-OBIM users. DHS security specifications also require auditing capabilities that log each user's activity 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 the OBIM systems employ auditing measures and technical safeguards to prevent the misuse of data.

Redress

This update does not concern how access, redress, and correction may be sought through USCIS. 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 (LPR), 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 the Freedom of Information Act (FOIA) unless disclosure is prohibited by law, or the agency reasonably foresees that disclosure would harm an interest protected by an exemption. If an individual would like to file a Privacy Act or Freedom of Information Act request to view their USCIS record, they may visit https://www.uscis.gov/records/request-records-through-the-freedom-of-information-act-or-privacy-act or mail the request to the following address:

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 Freedom of Information Act because information may contain law enforcement sensitive information, the release of which could possibly compromise ongoing criminal investigations. Further information about Privacy Act and Freedom of Information Act requests for USCIS records is available at http://www.uscis.gov. Any person, regardless of immigration status, may visit a local USCIS Field

[40] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE IMMIGRATION BENEFITS BACKGROUND CHECK SYSTEMS (IBBCS), DHS/USCIS/PIA-033 (2010), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

Office to identify and amend inaccurate records with supporting evidence. To find a local Field Office, individuals may visit: https://www.uscis.gov/about-us/find-a-uscis-office/fieldoffices.

Separate from the USCIS processes identified above, OBIM also provides processes for individuals to access and amend records that are contained in the Automated Biometric Identification System. Individuals can request access to their records by contacting:

OBIM Freedom of Information Act (FOIA) Officer
U.S. Department of Homeland Security
245 Murray Drive, SW
Washington, D.C. 20598-0675

Requests for information are evaluated to ensure that any release of information is lawful; will not impede an investigation of an actual or potential criminal, civil, or regulatory violation; and will not reveal the existence of an investigation or investigative interest on the part of DHS or another agency. Access may be limited pursuant to exemptions asserted under 5 U.S.C. § 552a(j)(2) and (k)(2) for the Automated Biometric Identification System.

Individuals, regardless of citizenship, can submit redress requests online through the DHS Traveler Redress Inquiry Program (TRIP) website, www.dhs.gov/trip, or mail the completed form and documents to:

DHS Traveler Redress Inquiry Program (TRIP)
601 South 12th Street
TSA-901
Arlington, VA 20598-6901

Any individual can request access to or correction of their personally identifiable information regardless of their nationality or country of residence. This process has been described in the DHS Traveler Redress Inquiry Program Privacy Impact Assessment[41] and information is available in multiple places on DHS's public website. Redress requests that come to the Traveler Redress Inquiry Program where a traveler encountered difficulties at a Point of Entry (POE) due to information in the Automated Biometric Identification System that needs to be modified or updated, are assigned via the Traveler Redress Inquiry Program to OBIM. OBIM then takes appropriate actions to the Automated Biometric Identification System record (if warranted) and makes that notation in the Traveler Redress Inquiry Program.

After an individual submits a redress form, the individual will receive notification of receipt from the DHS Traveler Redress Inquiry Program. The DHS Traveler Redress Inquiry Program will review the redress form and will determine which component/agency will be able to

[41] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE DHS TRAVELER REDRESS INQUIRY PROGRAM (TRIP), DHS/ALL/PIA-002 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

respond most effectively to the submission. When a redress request is related to OBIM processing, the DHS Traveler Redress Inquiry Program will coordinate with OBIM. OBIM will then review the individual's records and correct the information, if appropriate. DHS Traveler Redress Inquiry Program will notify the individual of the resolution of that request. Additionally, an individual may submit redress requests directly to the OBIM Privacy Officer. If an individual is dissatisfied with the response to their redress inquiry, then they can appeal to the DHS Chief Privacy Officer, who reviews the appeal and provides final adjudication concerning the matter. The DHS Chief Privacy Officer can be contacted at:

Chief Privacy Officer
Attn: DHS Privacy Office
U.S. Department of Homeland Security
Mailstop 0655
245 Murray Lane
Washington, D.C. 20528, USA

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 a wide range of security and privacy requirements (e.g., administrative, operational, and technical controls) that USCIS uses to protect data in accordance with federal security guidelines.[42] The Amazon Web Services Cloud is Federal Risk and Authorization Management Program (FedRAMP)-approved and authorized to host personally identifiable information.[43] 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 data's confidentiality, integrity, and availability, 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 also require auditing capabilities that log each user's activity 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

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

accessed. All USCIS systems employ auditing measures and technical safeguards to prevent data misuse.

USCIS is responsible for all personally identifiable information contained in CPMS, whether on USCIS infrastructure or a vendor's infrastructure. Therefore, it imposes strict requirements on vendors for safeguarding personally identifiable information. 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.[44]

All USCIS users and contractors are required to complete annual privacy and computer security awareness training to ensure their understanding of the 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 attend quality assurance calibration sessions. The USCIS Office of Privacy maintains a record of certificates of training for all users.

Further, OBIM secures the Automated Biometric Identification System and its data by complying with the requirements of DHS information technology security policy, particularly DHS 4300A Sensitive Systems Handbook. The Automated Biometric Identification System is periodically evaluated to ensure it complies with these security requirements. The Automated Biometric Identification System provides audit trail capabilities to monitor, log, and analyze system transactions, as well as actions and system accesses of authorized Automated Biometric Identification System users. As the Automated Biometric Identification System contains data from various sources, collected for a variety of uses, it is necessary to institute controls so that only those individuals with a need to know can access that data. The Automated Biometric Identification System has robust access controls, including role-based access and interfaces, which limit individual access to the appropriate discrete data collections. Misuse of the data in the Automated Biometric Identification System is mitigated by requiring that Automated Biometric Identification System users conform to appropriate security and privacy policies, follow established rules of behavior, and be adequately trained regarding the security of their systems. Also, a periodic assessment of physical, technical, and administrative controls is performed to enhance accountability and data integrity. External connections must be documented and approved with both parties' signatures in an interconnection security agreement (ISA), which outlines controls to protect the confidentiality, integrity, and availability of the information being shared or processed.

[44] *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

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

____
Deborah T. Fleischaker
Chief Privacy Officer (A)
U.S. Department of Homeland Security
privacy@hq.dhs.gov