Privacy Impact Assessment

for the

CBP Portal (e3) to EID/IDENT

DHS Reference No. DHS/CBP/PIA-012(d)

November 4, 2024

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) operates the e3 portal ("e3") to collect and transmit data related to law enforcement activities to the U.S. Immigration and Customs Enforcement (ICE) Enforcement Integrated Database (EID)[1] and the DHS Automated Biometric Identification System (IDENT) and its successor, the Homeland Advanced Recognition Technology System (HART).[2] CBP uses e3 to collect and transmit biographic, apprehension, and biometric data of individuals apprehended by U.S. Border Patrol (USBP). CBP is updating this Privacy Impact Assessment (PIA) to notify the public and assess the privacy risks of recent enhancements to e3. CBP will now use the e3 Biometrics module and Photo Service to take new photographs of individuals at the time of encounter and conduct facial photograph-based queries against derogatory photographs within CBP holdings. Additionally, CBP is launching a Mobile Intake application that allows users to begin the e3 intake process in the field.

Overview

U.S. Border Patrol agents enforce immigration and customs laws between the ports of entry by detecting, interdicting, and apprehending those who attempt to illegally enter or smuggle individuals or contraband, as well as preventing the entry of terrorists and terrorist weapons from entering the United States. As the primary transactional system used by U.S. Border Patrol agents to record apprehensions, the e3 portal was initially established to generate immigration enforcement forms, capture signatures from U.S. Border Patrol agents and individuals in custody, capture narratives entered by U.S. Border Patrol agents, and transmit biographic information for storage in ICE's Enforcement Integrated Database and biometric information for storage in the Automated Biometric Identification System and its successor, the Homeland Advanced

[1] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), DHS/ICE/PIA-015 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice; and DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 89 Fed. Reg. 55638 (July 5, 2024), *available at* https://www.dhs.gov/system-records-notices-sorns.

[2] *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. The Homeland Advanced Recognition Technology System is replacing the legacy IDENT 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 specific positions of public trust; and associated testing, training, management reporting, planning and analysis, development of new technologies, and other administrative uses. For more information on IDENT, *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), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

Recognition Technology System. e3 consists of several modules detailed in previous versions of this Privacy Impact Assessment.

U.S. Border Patrol agents use the existing e3 Biometrics module to store and transmit biographic information to the Enforcement Integrated Database and biometric information to the Automated Biometric Identification System/Homeland Advanced Recognition Technology System for processing, identification, and verification of identity of individuals encountered or apprehended. Historically, these biometric checks have been fingerprint-based. The e3 portal transmits biographic and biometric data in real-time to the above systems and retrieves records from those systems for identity verification and CBP enforcement action purposes. The e3 portal relies on data within the Enforcement Integrated Database and the Automated Biometric Identification System/Homeland Advanced Recognition Technology System to populate all query responses and serves as a method for U.S. Border Patrol agents to view returns from system queries.

U.S. Border Patrol submits biometrics-based queries that include fingerprint, photograph, or iris to query IDENT/Homeland Advanced Recognition Technology (HART) Systems and other interoperable federal biometrics systems: the Department of Defense (DOD) Automated Biometric Information System (ABIS)[3] and the Federal Bureau of Investigation (FBI) Next Generation Identification (NGI).[4] Following a match to an existing fingerprint in those systems, they will return any corresponding biographic information, and any photographs, associated with the probe[5] fingerprint to e3. e3 then displays the photos and fingerprint data in e3 interfaces, forms, and reports. Photo Service automatically retrieves photos and fingerprints from the above sources and displays the consolidated responses within a unified user interface. This capability allows the U.S. Border Patrol agent to evaluate and process photos and fingerprints from an apprehended individual without logging into each biometric application above, which enables the agent to identify or verify the identity of the apprehended individual quickly.

Reason for the PIA Update

CBP is updating the e3 Privacy Impact Assessment series to provide transparency to the public and assess the privacy risks associated with changes to the Unified Processing Mobile Intake and the e3 Photo Service modules, which permit U.S. Border Patrol agents to biometrically search, identify, and enroll individuals from the field into various systems. With this update, the

[3] *See* Privacy Impact Assessment (PIA) for the Department of Defense Automated Biometrics Identification System (DoD ABIS), *available at* http://ciog6.army.mil/Portals/1/PrivacyImpactAssessments/2015/DoD%20ABIS.pdf.

[4] For more information about the FBI's Next Generation Identification (NGI), *see* https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/interstate-photo-system.

[5] A probe fingerprint or photograph is the biometric used to query other biometrics to determine whether the probe biometric matches any existing biometrics within holdings.

U.S. Border Patrol is conducting biometric-based searches using a newly collected probe *photograph* in addition to the longstanding fingerprint-based queries described above.

e3 now leverages the internal CBP facial matching technology, known as the Traveler Verification Service (TVS),[6] to conduct biometric queries using facial recognition technology. Using a new encounter photograph for all individuals apprehended by the U.S. Border Patrol, CBP will now conduct facial photograph-based queries against derogatory photographs within CBP holdings, along with the traditional fingerprint-based biometric checks.

Historically, U.S. Border Patrol agents used workstations in a physical sector or station location to view and input information into e3. However, the U.S. Border Patrol often apprehends individuals in remote locations; sometimes several hours' drive from the nearest U.S. Border Patrol physical location. By enabling mobile intake and biometric searching against derogatory information, U.S. Border Patrol agents can identify potentially violent or wanted individuals in the field, without traveling to a physical U.S. Border Patrol location. Mobile intake, biometric query, and facial recognition identification in the field reduces processing time and promotes agent safety by enabling U.S. Border Patrol agents to identify and take precautions with potentially violent individuals immediately.

1. Mobile Intake Application

CBP has implemented a new Mobile Intake application that enables U.S. Border Patrol agents to capture the individual's information at the time of apprehension in the field through a government-issued mobile device. U.S. Border Patrol agents using the Mobile Intake application may electronically record biographic information (e.g., name, date of birth, age, sex, country of birth, citizenship), biometric information (e.g., individual's photo), document information (e.g., document number, issuing country, document type), and property information (e.g., property tag number) to create a new Tracking, Sign-cutting, and Modeling (TSM)[7] event (if one exists) at the time of apprehension, which will then generate an e3 event number.

Using the Mobile Intake application, authorized users begin by capturing a new facial photograph of the apprehended individual. This image is stored locally on the U.S. Border Patrol mobile device and sent to the Traveler Verification Service, as discussed below. The probe image

[6] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TRAVELER VERIFICATION SERVICE (TVS), DHS/CBP/PIA-056 (2018), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[7] The Tracking, Sign-cutting, and Modeling (TSM) application stores and displays illegal border-crossing and interdiction activity; specifically, the system stored information regarding agent tracking efforts, sensor activations, and reports related to potential unlawful border crossings. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE INTELLIGENT COMPUTER ASSISTED DETECTION (ICAD) SYSTEM, DHS/CBP/PIA-075 (2022), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

is stored on the U.S. Border Patrol agent's mobile device for the duration of the agent's shift and no more than ten hours from the time of submission on that local device.

The Traveler Verification Service is *only searching against derogatory photographs within CBP holdings.*[8] If the search identifies a match, the biographic information associated with the matched image will be used to populate the individual's details page. This information will also indicate the reason the photograph is considered derogatory, such as whether the individual has an active warrant, prior apprehensions, or has a nexus to terrorism or transnational organized crime.

Following the photograph-based query, Mobile Intake displays potential photographic matches to the U.S. Border Patrol agent performing the intake. The U.S. Border Patrol agent will be able to select one of the matches, if any, to populate the biographic data in the new e3 apprehension event following a positive match determination. Any match meeting a certain threshold match score is displayed within the Mobile Intake application, which passes the results back to e3 Intake, and ultimately the U.S. Border Patrol agent processing the individual. The match-scoring system is not absolute and identifications are not made on the score alone. A U.S. Border Patrol agent must review all matches and any additional available data when determining a positive match.

If the individual has any identification documents (such as passports, driver's licenses, birth certificates, or voter registration cards), the U.S. Border Patrol agent will attempt to use the optical character recognition capabilities[9] to scan and parse the document information and populate the individual's biographic data in e3. If the apprehended individual has a prior apprehension event *and* an identification document, the biographic data from the identification document will be used in the new e3 event.

The new probe photograph and any subsequent match photographs and subject biographic information (based on the matches) are stored locally in the "history" screen of the Mobile Intake application. The e3 system is transitioning to a new processing system called "Unified Processing" which will share a platform and backend storage system with the Office of Field Operations encounter processing system, Unified Secondary.[10] The photographs processed through Mobile Intake are stored in the same large gallery as the Unified Secondary photographs, both of which will eventually populate the future Unified Processing system. A Privacy Impact Assessment for

[8] For more information about the facial matching process and the Traveler Verification Service, please *see* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TRAVELER VERIFICATION SERVICE (TVS), DHS/CBP/PIA-056 (2018), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[9] Optical character recognition is the process that converts an image of text into a machine-readable text format.

[10] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR U.S. CUSTOMS AND BORDER PROTECTION UNIFIED SECONDARY, DHS/CBP/PIA-067 (2020), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

Unified Processing is forthcoming and deployment of the Unified Processing system will not commence until the Privacy Impact Assessment is published.

2. Enhanced e3 Federated Person Query 2 (FPQ2) Application[11]

In 2020, CBP published an e3 Privacy Impact Assessment series update to describe the new e3 Photo Service. The e3 Photo Service replaced the existing e3 photograph and fingerprint retrieval capability to display responsive photographs and fingerprints within e3 user interfaces, forms, and reports. The e3 Photo Service (in conjunction with the e3 NextGen application and e3 Biometrics) retrieves photos and fingerprints through a query and response from the DOD Automated Biometric Information System and the FBI Next Generation Identification. The Automated Biometric Identification System/Homeland Advanced Recognition Technology System displays the photos and fingerprint data in e3 interfaces, forms, and reports. e3 Photo Service automatically retrieves photos and fingerprints from the above sources and displays the consolidated responses within a unified user interface. Since 2020, CBP has accessed prior apprehensions or encounters via the e3 Photo Service.

For this Privacy Impact Assessment update, CBP is expanding the e3 Photo Service to include the Traveler Verification Service within the e3 Federated Person Query 2 application to conduct facial recognition for identification purposes for all individuals between the ages of 14 to 79 who are apprehended by U.S. Border Patrol. In addition to the traditional biometric identification checks using fingerprints (described in the 2020 e3 Photo Service Privacy Impact Assessment), CBP will now use the Traveler Verification Service as part of the e3 enrollment process for all apprehended individuals within the appropriate age range. CBP will take a new photograph of all appropriate apprehended individuals and will leverage the Traveler Verification Service to search CBP photo repositories containing galleries of derogatory images in CBP holdings to identify individuals who may be a threat to officer safety, pose a potential security concern, or warrant additional scrutiny based on facial recognition technology and agent training.

The results will include the photograph and any biographic information associated with the individual, including information about previous apprehensions. Upon receiving a positive match, the U.S. Border Patrol agent must ensure proper adjudication of the match prior to the transfer or release of the individual. Generally, the individual will remain in U.S. Border Patrol custody until the match has been adjudicated and a custodial decision and processing pathway has been determined. Pursuant to CBP policy, CBP must make every effort to hold noncitizens for the least amount of time required for their processing, transfer, release, or repatriation as appropriate and

[11] For more information on CBP's use of facial recognition technologies, and any subsequent enhancements to the e3 Federated Person Query 2 Application, please refer to the forthcoming CBP Law Enforcement Use of Facial Recognition Technologies Privacy Impact Assessment, which will be *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

operationally feasible. CBP generally should not hold individuals in custody for longer than 72 hours in CBP hold rooms or holding facilities.[12]

CBP uses any derogatory information found during these queries to determine how to process the apprehended individual, and populate appropriate e3 forms related to the individual. Any derogatory data retrieved and matched to an individual in U.S. Border Patrol custody is stored in e3. The Traveler Verification Service search results will remain associated with the e3 record and can be reviewed at any time by searching for the individual again. The results include the photograph and any biographic information associated with the individual including information about previous apprehensions.

The enhanced e3 Federated Person Query 2 application will query the following Traveler Verification Service prior apprehensions and derogatory photo repositories:

- *Watch List Service (WLS):*[13] The Watch List Service is a copy of the Terrorist Screening Database (TSDB), the U.S. Government's consolidated database maintained by the Department of Justice (DOJ) FBI Terrorist Screening Center (TSC). The DHS Watchlist Service maintains a synchronized copy of the Terrorist Screening Database, which contains personally identifiable information (PII) and disseminates Terrorist Screening Database records it receives to authorized DHS Components.
- *TECS Lookout records:*[14] CBP or other TECS partner agencies, may create a TECS Lookout record. Lookout records are made based on law enforcement, anti-terrorism, travel document fraud, or other interests (for example, if a traveler to a medical outbreak area posed a public health threat). Such interests are based on previous violations of law, suspicion of violations, or a business or occupation in which the law enforcement community has an interest. TECS lookout records created by external agencies are considered under the control of CBP, with a nexus to border security, because they are used by CBP Officers at primary and secondary inspection processing at the ports of entry.
- *Foreign Encounters*, which include:

[12] *See* Homeland Security Act at 6 U.S.C. 211(m) and CBP's National Standards on Transport, Escort, Detention and Search (TEDS), *available at* https://www.cbp.gov/document/directives/cbp-national-standards-transport-escort-detention-and-search.

[13] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE WATCHLIST SERVICE, DHS/ALL/PIA-027 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

[14] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING (TECS) NATIONAL SAR INITIATIVE, DHS/CBP/PIA-009 (2010 and subsequent updates); AND THE TECS SYSTEM: PLATFORM, DHS/CBP/PIA-021 (2016 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

- **Biometric Identification Transnational Migration Alert Program (BITMAP)**,[15] which is a comprehensive information-sharing ICE program, designed to strengthen the international cooperation and coordination of law enforcement agencies' efforts to combat transnational criminal activity, enhance border security, and enforce customs and immigration laws. The Biometric Identification Transnational Migration Alert Program leverages biometric and biographic information collected and shared by foreign partners, logistically capable of identifying foreign nationals within the host country's geographic borders reasonably suspected to be or involved in criminal activity that poses an immigration, criminal, or international security risk.
- **Biometric Data Sharing Program (BDSP)**,[16] which supports the exchange of biometrics and associated biographic information between a foreign government and DHS.
- **Foreign Border Crossing Records (FBCR)**,[17] which provides the ability to collect, compare, and analyze traveler data to help the country secure its borders or other controlled areas.

Data collected through the Mobile Intake application is populated in e3 Next Gen and e3 Biometrics, which links the apprehension event to the Tracking, Sign-cutting, and Modeling event. All information is ultimately stored in the Enforcement Integrated Database.

Privacy Impact Analysis

Authorities and Other Requirements

The legal authorities for CBP's collection, use, maintenance, and dissemination of information within the e3 portal have not changed since the original Privacy Impact Assessment in 2012 and updated Privacy Impact Assessments in 2017, 2020, and 2021. The Border Patrol Enforcement Records (BPER) System of Records Notice (SORN)[18] covers CBP's collection of information on individuals whom it encounters, apprehends, detains, or removes in relation to border crossings, checkpoint operations, law enforcement actions, and other operations related to

[15] The forthcoming ICE Biometric Identification Transnational Migration Alert Program Privacy Impact Assessment will analyze how ICE uses biometric and biographic data and describe the exchange of information between ICE and its law enforcement partners, in a manner that safeguards legal rights, civil liberties, and privacy rights in accordance with law, regulation, and policy.

[16] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE INTERNATIONAL BIOMETRIC INFORMATION SHARING PROGRAM (IBIS), DHS/ALL/PIA-095(A) (2022 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

[17] Formerly known as Personal Identification Secure Comparison and Evaluation System (PISCES).

[18] *See* DHS/CBP-023 Border Patrol Enforcement Records System of Records (BPER), 81 Fed. Reg. 72601 (October 20, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

the enforcement of the Immigration and Nationality Act (INA) and related authorities. This information may include biographic, biometric, geolocation data, and enforcement-related information.

The Border Patrol Enforcement Records System of Records Notice provides coverage for CBP's maintenance of records in e3. Biometric data, including derogatory photographs and underlying biographic information, stored in the Automated Targeting System (ATS) is covered by the source System of Records Notices (if applicable) or the Automated Targeting System System of Record Notice,[19] and records associated with a law enforcement action are stored in accordance with the TECS System of Records Notice.[20]

Characterization of the Information

CBP uses e3 to collect biographic and biometric data, encounter information, health condition and medication information, information related to border violence, and prosecution-related data obtained from individuals during DHS enforcement encounters. A complete list of these data elements is available in the 2012, 2017, 2020, and 2021 e3 Privacy Impact Assessments and can be referenced in Appendix A.

With the exception of the expanded use of photo matching repositories, there is no additional personally identifiable information collected, generated, or retained in association with the updates documented in this Privacy Impact Assessment.

Privacy Risk: There is a risk that the facial images collected through the Traveler Verification Service process will not be of high enough quality or be an accurate representation, therefore negatively impacting the reliability of the matching service.

Mitigation: This risk is mitigated. Should any issues with picture quality occur, the individual may be taken to the physical sector or station for facial collection.

Further, CBP is fully committed to testing new processes and capabilities for using facial recognition technology. CBP currently uses an internal facial recognition technology through the Traveler Verification Service. CBP is continually testing and evaluating the accuracy of the camera technology and the Traveler Verification Service algorithms. CBP has submitted the Traveler Verification Service algorithms to the National Institute for Standards and Technology (NIST) for ongoing testing to ensure the highest match rates and match score confidence. In addition, DHS Science & Technology (S&T) tests the effectiveness of commercial, academic, and government algorithms in matching facial images. S&T identifies how each algorithm performed as a true positive rate, false positive rate, false match rate, and false non-match rate. CBP continues to

[19] *See* DHS/CBP-006 Automated Targeting System, 77 Fed. Reg. 30297 (May 22, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.

[20] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 Fed. Reg. 77778 (December 19, 2008), *available at* https://www.dhs.gov/system-records-notices-sorns.

partner with S&T, OBIM, and NIST to evaluate the Traveler Verification Service algorithms and test biometric technologies developed by specified vendors to ensure CBP always relies on the most accurate algorithms with the least likelihood for bias.

Uses of the Information

CBP's use of the information within e3 has remained the same since the original Privacy Impact Assessment publication. CBP continues to process biographic, biometric, encounter, and border violence data through e3 to document CBP actions to ensure border security.

The recent enhancements to e3 help decrease the amount of time it takes a U.S. Border Patrol agent to process an apprehended individual and helps expedite the transfer of custody from CBP. In addition, they are providing possible derogatory information to the U.S. Border Patrol agent while in the field which helps to increase officer safety.

Privacy Risk: There is a risk that CBP will use a positive facial recognition match to take law enforcement action against an individual.

Mitigation: This risk is mitigated. CBP does not take any adverse action based on facial recognition match alone. A U.S. Border Patrol agent must review all matches and any additional available data when making a positive match determination. Upon receiving a positive match, the U.S. Border Patrol agent must ensure proper adjudication of the match prior to the transfer or release of the individual. Ultimately, the individual will remain in U.S. Border Patrol custody until the match has been adjudicated and a custodial decision and processing pathway has been determined. Pursuant to CBP policy, CBP must make every effort to hold noncitizens for the least amount of time required for their processing, transfer, release, or repatriation as appropriate and operationally feasible. CBP generally should not hold individuals in custody for longer than 72 hours in CBP hold rooms or holding facilities.[21]

Notice

All persons the U.S. Border Patrol apprehends, including those attempting to enter the United States unlawfully, as well as those who are otherwise subject to removal, are subject to data collection requirements and processes that include providing biometric data and the collection of limited medical health information. Operational and logistical considerations prevent individuals encountered between ports of entry from receiving advanced notice of the data collection. This Privacy Impact Assessment, as well as the Homeland Advanced Recognition Technology System Privacy Impact Assessment; Enforcement Integrated Database Privacy Impact Assessments; Traveler Verification Service Privacy Impact Assessment; Automated Targeting System Privacy

[21] See Homeland Security Act at 6 U.S.C. 211(m) and CBP's National Standards on Transport, Escort, Detention and Search (TEDS), *available at* https://www.cbp.gov/document/directives/cbp-national-standards-transport-escort-detention-and-search.

Impact Assessments; and Border Patrol Enforcement Records System of Records Notice provide notice to all persons about these CBP collections.

Privacy Risk: There is a risk that individuals apprehended in the field by the U.S. Border Patrol will not be aware that CBP is using facial recognition to vet them against derogatory information.

Mitigation: This risk is partially mitigated. This Privacy Impact Assessment provides specific public notice of how U.S. Border Patrol uses facial recognition to improve the identification of individuals who pose a potential security concern or warrant additional scrutiny. Further, CBP will have the individual in custody when taking a probe photo, so there will be some awareness from the individual that their image is being captured by CBP.

In addition, CBP remains transparent about its uses of facial recognition for identity verification and biometric vetting purposes through multiple Privacy Impacts Assessments, public statements, Congressional testimony, and various oversight audits and reviews.

Data Retention by the Project

The newly collected probe photograph is stored locally on the U.S. Border Patrol agent's mobile device for the duration of the agent's shift, and no more than ten hours from the time of submission. The new probe photograph and any subsequent match photographs and subject biographic information (based on the matches) are stored locally in the "history" screen of the Mobile Intake application.

The e3 system is transitioning to a new processing system called "Unified Processing" which will share a platform and backend storage system with the Office of Field Operations encounter processing system, Unified Secondary.[22] The photographs processed through Mobile Intake are stored in the same large gallery as the Unified Secondary photographs, both of which will eventually populate the future Unified Processing system. A Privacy Impact Assessment for Unified Processing is forthcoming.

The retention schedule for biographic and biometric encounter records remains 75 years. There are no other changes to retention.

Privacy Risk: There is a risk that the U.S. Border Patrol will retain the probe photograph locally on the Agent's mobile intake device for a period that is longer than necessary to accomplish a CBP mission.

Mitigation: This risk is mitigated. The probe photograph is only stored locally within the Agent's mobile intake session history within the Mobile Intake application. The picture is stored

[22] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR U.S. CUSTOMS AND BORDER PROTECTION UNIFIED SECONDARY, DHS/CBP/PIA-067 (2020 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

locally as a short-term backup in the event of poor signal or inability to upload the whole encounter from the field, and is automatically deleted at the end of the Agent's shift or after no longer than 10 hours. In addition, it allows the Agent to scroll through his or her encounters for the day when completing and verifying any end-of-shift processing documentation.

Information Sharing

There are no changes to information being shared because of this update. The U.S. Border Patrol has always shared this information with ICE and other stakeholders as part of the immigration enforcement process.

Redress

There are no changes to redress because of this update.

Auditing and Accountability

There is no change to auditing and accountability because of this update.

Responsible Officials

Courtney T. Ray
Director
Strategic Planning and Analysis Directorate
U.S. Border Patrol
U.S. Customs and Border Protection

Debra L. Danisek
Privacy Officer
Privacy and Diversity Office
Office of the Commissioner
U.S. Customs and Border Protection
Privacy.CBP@cbp.dhs.gov

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

APPENDIX A: LIST OF DATA ELEMENTS

e3 Privacy Impact Assessment, dated July 2012 & updated 2017

Biographic data includes:

- Name
- Aliases
- Data of birth
- Phone numbers
- Addresses
- Nationality
- Social Security Number
- A-Number
- Employment history
- Educational history
- Immigration history
- Criminal history

Biometric data includes:

- Height
- Weight
- Eye color
- Hair color
- Fingerprints
- Iris scans (collected as part of the pilot program)
- Photographs

Encounter data includes:

- Location of apprehension/encounter
- Name, place of birth, date and time of apprehension

- Citizenship
- Matches to Information in screening databases
- Identification numbers of documents found on the individual including but not limited to USCIS Benefit Number; State ID number; A-Number; Travel Document Number
- Fingerprint Identification Number (FIN) Violations

Border violence data includes:

- Name of Agent
- Assailant's Information
- Injury descriptions
- Hospital names and locations
- Witness accounts and information
- Weapon descriptions

Prosecutions data includes:

- Charges
- Case dates
- Verdicts
- Subject information
- Attorney information
- Judge information
- Sentencing information
- Release dates

e3 Privacy Impact Assessment, updated July 2020

SID pilot: The only new information CBP generates and retains for the SID pilot is the barcode that is printed on the wristband.[23] In order to associate an e3 record with a person, CBP is placing a barcode on a wristband worn by an individual and retaining the barcode number in e3.

CBP Form 2500, *Alien Initial Health Interview Questionnaire:*

- Subject Name
- A-Number
- Event Number
- Date of Birth
- Gender
- Country of Citizenship or Last Habitual Residence
- Name of USBP Agent
- Medical Information based on self-reported medical issues and USBP agent observations such as medical or mental health issues, medications taken, allergies, drug use, pregnancy, injuries, rashes, and diseases.

CBP Form 93, *CBP Unaccompanied Alien Child (UAC) Screening Addendum:*

- Individual's Name
- A-Number
- Date of Birth
- Gender
- Country of Citizenship
- Country of Habitual Residence
- USBP Agent Name

[23] A forthcoming Privacy Impact Assessment for the Amenities, Property, and Identification Program (APIP) will be *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection. It will discuss the use of barcodes and wristbands to track the location of property and individuals in CBP custody.

- Responses to questions regarding the USBP agent's assessment of UAC ability to make an independent decision; UAC responses to screening questions regarding fear-of-return, intimidation, labor and sex trafficking.

DOJ Request for National DNA Database Entry Form (DOJ Form FD-936)

The table below lists all data points required to complete DOJ Form FD-936, specifying which data fields already exist in EID and which CBP needs to collect via e3.

Required Fields	
Existing e3 Fields	**New e3 Fields**
Agency Name (e.g., CBP)	Master Name (i.e., the original name connected to an FBI Identity History Summary)
Originating Agency Identifier	Next Generation Identification (NGI)[24]
Agency Address (city, state, zip code)	Collection Device Identifier (i.e., barcode)
Agency Phone Number	Collection Date/Time (YYYY/MM/SS/HH:MM:SS)
Subject Last Name	DNA Collection Exemption Reasons
Subject First Name	
Subject Middle Name	
FBI Universal Control Numbers (UCN)	
Subject Date of Birth (YYYYMMDD)	
Gender	
Race/Ethnicity	
A-Number	
Social Security number	

[24] *See* NGI Privacy Impact Assessment, available at https://www.fbi.gov/services/information-management/foipa/privacy-impactassessments.

DHS Fingerprint Identification Number (DHS FIN)	
Passport Number	
Arrest/Conviction Code	
Collector Last Name (CBP Employee)	
Collector First Name (CBP Employee)	
Event # / TECS Subject Record ID#	

e3 Privacy Impact Assessment, updated August 2021

COVID 19 Survey

USBP agents attempt to identify whether encountered individuals in CBP custody may have the COVID-19 virus. Agents accomplish this by observing and interviewing individuals while in CBP custody, completing additional COVID-19 questions during the initial medical health screening process, and completing the CBP Form 2500, *Alien Initial Health Interview Questionnaire.*[25] The information is used by USBP agents to determine appropriate custodial arrangements (such as for juveniles or individuals requiring medical care) and the need for additional medical observation or treatment.

USBP agents may observe, and interview encountered individuals and answer the following questions in e3 during the intake process.

- Has the encountered individual traveled to/through/from an at-risk country within the last 14 days? Yes/No
- Does the encountered individual exhibit any symptoms (fever, cough, difficulty breathing, or other flu-like symptoms)? Yes/No
- Was the CDC consulted regarding the encountered individual? Yes/No (Any consultation with the CDC is done verbally. No information is transmitted to the CDC.)
- Was the encountered individual referred to a hospital for any flu-like symptoms? Yes/No
- Was the encountered individual segregated and monitored as a precaution? Yes/No
- Was the encountered individual quarantined as per the CDC? Yes/No
- Was the encountered individual transferred to ICE? Yes/No
- Was the encountered individual released? Yes/No
- Was the encountered individual tested for COVID-19? Yes/No
- If encountered individual is tested for COVID-19, was the test positive? Yes/No

[25] The purpose of CBP Form 2500 is to provide initial identification of medical issues that may require immediate CBP referral to 911/EMS/the local hospital or to identify potential medical issues that may require a more detailed medical assessment by a trained medical professional.