Privacy Impact Assessment Update
for the

CBP Portal (e3) to EID/IDENT

DHS/CBP/PIA-012(a)

August 9, 2017

Contact Point
Antonio J. Trindade
Strategic Planning and Analysis Directorate
U.S. Border Patrol
U.S. Customs and Border Protection
(202) 344-1446

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

Abstract

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) operates the e3 portal, which serves as the CBP portal to the U.S. Immigration and Customs Enforcement's (ICE) Enforcement Integrated Database (EID) and the DHS Automated Biometric Identification System (IDENT) to collect and transmit data related to law enforcement activities. e3 collects and transmits biographic, encounter, and biometric data for identification and verification of individuals encountered at the border for CBP's law enforcement and immigration mission. CBP is updating this Privacy Impact Assessment (PIA) to notify the public of enhancements to e3 impacting personally identifiable information (PII), including: the collection of iris images; a new module for custodial tracking and management; new system search functionality; and new information sharing arrangements.

Overview

CBP uses the e3 portal (e3) to transmit and store data to ICE's EID[1] and DHS's IDENT[2] for processing, identification, and verification of individuals encountered or apprehended at the border. e3 transmits data in real time from CBP Border Patrol Agents to ICE EID and IDENT, and retrieves records from those systems for CBP enforcement action purposes. The e3[3] suite of applications, which communicate with each other over the CBP network and through EID, which is owned by ICE, enables CBP Border Patrol Agents to record an apprehended individual's biographic information and seized property; uniquely identify or verify the identity of the individuals they encounter by capturing the apprehended individual's photograph and fingerprints and transmitting them in real-time to IDENT; facilitate the capture and recording of data pertaining to border violence and alien smugglers; view and record information pertaining to criminal trials; build cases for prosecution; generate documents electronically per the requirements of a particular court; print, update, and track cases; and create statistical reports.

Reason for the PIA Update

CBP is updating the e3 PIA to document changes since the original e3 PIA was published in 2012, including: (1) system enhancements and upgrades for user efficiency; (2) expanded

[1] *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID) and associated updates, *available at* www.dhs.gov/privacy, and DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 FR 72080 (October 19, 2016).
[2] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System, *available at* www.dhs.gov/privacy.
[3] *See* DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT, *available at* www.dhs.gov/privacy, and DHS/CBP-023 Border Patrol Enforcement Records System of Records (BPER), 81 FR 72601 (October 20, 2016).

collection of iris images; (3) modifications that enable CBP to track the location of individuals in its custody; and (4) enhanced user query capabilities.

System Enhancements

This PIA documents several new e3 modules used for existing functions, and several updates to existing modules:

- **e3 Homepage**: The new e3 Homepage Module provides an interface that allows CBP Border Patrol Agents quick access to the e3 operational modules and announcements from CBP and U.S. Border Patrol (USBP) Headquarters and the Office of Information and Technology (OIT) to quickly disseminate outage, release, announcements, and training information directly to CBP Border Patrol Agents in the field.
- **e3 Intake**: The e3 Intake Module, an enhancement to the Processing and Biometrics modules, allows CBP Border Patrol Agents to quickly create a new record in e3 and subsequently in EID. This allows CBP Agents and Officers to generate a record of the subject in the e3 Detentions Module for custodial tracking purposes, and conduct a biometric identity verification and records check analysis via the e3 Biometrics Module.
- **e3 Mobile**: The new e3 Mobile Module combines the functionalities of the e3 Intake and the e3 Biometrics Module providing CBP Border Patrol Agents with the ability to create new records and input subject biographical and biometric data via a CBP-issued handheld device. The module is only accessible on the CBP intranet via a mobile browser[4] interface that has direct access to the CBP network or using a virtual private network (VPN) connection to the CBP network. This application can be used on a tablet and combined with a fingerprint scanner to enable CBP Border Patrol Agents to identify and assess the threat level of subjects in more remote locations (so they do not have to travel long distances back to the station to verify an individual's identity or run a records check). Where cell coverage exists, CBP Agents may use the module to begin the intake and field interview process and connect to EID and IDENT.
- **e3 Apprehension Log**: The new e3 Apprehension Log Module allows CBP Border Patrol Agents to query, filter, and review information in e3 on all apprehended subjects. For example, the CBP Agent or Officer can search on a date range, country of citizenship, and gender, and the system will display all subjects matching that criteria.
- **e3 Processing**: The existing e3 Processing Module has been updated to include minor enhancements to reflect operational workflow changes that do not substantively impact the collection or use of information within e3.

[4] A mobile browser interface is a browser that has been optimized to display the content on the small display screens of handheld computing devices, such as smartphones and tablets.

- **e3 Biometrics**: The existing e3 Biometrics Module has been updated to support multimodal biometrics technologies, particularly iris capture. CBP Border Patrol Agents capture and submit iris information of subjects in USBP custody to the DHS Office of Biometric Identity Management (OBIM) for storage in the IDENT system. CBP maintains ownership of these records despite their storage in the DHS biometric repository, IDENT.
- **e3 Prosecutions**: The existing e3 Prosecutions Module includes minor enhancements to support changes in operations as well as form updates to support requirements by federal courts, such as updating language for plea arrangements and including date of last deportation (at the request of some courts). All information was already available in EID; the enhancements permitted CBP to update cases and forms per the requirements of a particular court.
- **Operations Against Smugglers Initiative on Safety and Security (OASISS)**: The OASISS Module, which tracks and manages OASISS cases, was a joint venture between the United States and Mexico to promote information sharing and prosecution of suspected human traffickers and alien smugglers.

Several of the e3 Module enhancements reflect new collections or uses of PII. In addition to the system user interface enhancements, CBP has enhanced e3 to include the expanded collection of iris images and the ability to track detainees, discussed in full below.

Federated Person Query 2 and New System Interfaces

The new Federated Person Query 2 Module uses Web Services to facilitate the automatic retrieval of subject encounter data from multiple data systems, and displays the consolidated data with biometric data within a single unified user interface. The single unified interface[5] allows the CBP Agent or Officer to more quickly evaluate and process the subject without logging into other applications. The Federated Person Query enables e3 users to run biometric queries of IDENT (including both simple search and search and enroll), Federal Bureau of Investigation (FBI) Next Generation Identification (NGI) (including both simple search and search and enroll),[6] and the Department of Defense (DOD) Automated Biometric Information System (ABIS)[7] for criminal history and encounter information. Users can run biographic queries of CBP TECS,[8] FBI National

[5] To permit access across multiple applications, the single unified interface employs single sign-on functionality when a user first opens any e3 application. It uses the CBP Agents/Officers' information and checks those systems to see if the CBP Agent/Officer has access/update profiles, specifically for access to TECS and the NCIC, described later in the paragraph. The single unified interface is a consolidation of those systems.

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

[7] *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.

[8] *See* DHS/CBP/PIA-021 TECS System: Platform (August 2016), *available at* www.dhs.gov/privacy.

Crime Information Center (NCIC),[9] ICE ENFORCE Alien Removal Module (EARM),[10] and NLETS.[11] Permission to run the new Federated Person Query 2 are tied to the original system of record or a general CBP Agent and Officer role. For example, the CBP Agent or Officer will need to have access to the U.S. Department of Justice's (DOJ) Joint Automated Booking System (JABS)[12] in order to query and retrieve NGI, access to TECS to see TECS information, and access to NCIC to see the query/retrieve NCIC/NLETS data. CBP Border Patrol Agents need only a general CBP Agent or Officer permission role to query/retrieve EARM information.

In addition to the new query functionality, updates to e3 include two new system interfaces:

- e3 interfaces with CBP's Intelligent Computer Assisted Detection (ICAD) application suite through its dispatch functionality and through the Tracking, Sign-cutting, and Modeling (TSM) module, which USBP uses to identify potential patterns of illicit activity. Patterns of illicit activity are formed by linking the EID event number (including the apprehension and seizure date) with the TSM track or ICAD dispatch information.
- e3 interfaces with the CBP Seized Currency and Asset Tracking System (SEACATS).[13] SEACATS users may import certain e3 event data to facilitate the creation of seizure and other enforcement records.

Expanded Collection of Iris Images

The 2012 e3 PIA described and assessed a CBP pilot program involving the collection of iris images for submission to IDENT. The goal of the pilot was to evaluate how well this modality provided for identity verification and whether it was easily cross-referenced with the fingerprints and other multimodal biometric information on file.[14] CBP anticipated that the use of iris images would be beneficial since they could be collected more quickly, are more reliable, require less storage capacity and transmission, and can be conducted with less physical contact with the

[9] For more information about the FBI's National Crime Information Center (NCIC), please *see* https://www.fbi.gov/services/cjis/ncic.
[10] *See* DHS/ICE/PIA-015(b) Enforcement Integrated Database (EID) ENFORCE Alien Removal Module (EARM 3.0) (May 20, 2011), *available at* www.dhs.gov/privacy.
[11] The National Law Enforcement Telecommunications System (NLETS) is the International Justice and Public Safety Information Sharing Network: a state-of-the-art secure information sharing system for state and local law enforcement agencies. It provides electronic messaging to allow information exchange between state, local, and federal agencies and support services to justice-related programs. The network is operated by Nlets, a non-profit corporation owned and operation by the states and funded solely by fees for service. *See* http://www.nlets.org/.
[12] For more information about JABS, please *see* DOJ Joint Automated Booking System PIA, *available at* http://www.justice.gov/sites/default/files/jmd/legacy/2014/06/27/jabs.pdf and JUSTICE/DOJ-005 Nationwide Joint Automated Booking System (JABS), 72 FR 3410 (January 25, 2007).
[13] *See* DHS/CBP/PIA-040 Seized Assets and Case Tracking System (April 10, 2017), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[14] Existing multimodal biometric information includes, but is not limited to, descriptive information such as: height, weight, eye color, hair color, facial photograph, fingerprints, and iris scans.

subject.

Upon completion of the pilot, CBP found that iris images were beneficial and is expanding the use of this modality gradually as resources allow. Along with fingerprints, CBP's collection of iris images benefits CBP's ability to ensure accurate identity verification of individuals apprehended or encounter by CBP Border Patrol Agents. Iris collection enhances the accuracy of CBP's biometric holdings. Iris recognition tools look at 240 characteristics as opposed to even the most high-end fingerprint systems that measure approximately 40 to 60 characteristics. Iris recognition software has a false accept rate of approximately 1 in 1.2 million, whereas fingerprint false accept rate is approximately 1 in 100,000. Iris capture is fast and requires no physical contact, and an individual's iris is stable throughout a person's life. Fingerprinting takes longer and requires physical contact with a device and the devices require regular cleaning. And, based on occupation, trauma, or disease, individual fingerprints may be obscured, damaged, or changed.

Iris Collection Process

When U.S. Border Patrol Agents encounter individuals who are unlawfully entering the United States, or are subject to removal under the Immigration and Naturalization Act (INA), it is critical to identify who the subject is and determine whether that individual has been previously encountered and whether he or she is potentially a threat to officer safety or national security. To do so, Agents take the individual(s) to the local Station or Sector for processing and use the e3 Processing Module. As part of processing (intake), Agents capture ten (10) rolled fingerprints, a facial photograph, and an image of the subject's iris.

Iris is collected at the same time as the facial photograph, using a special camera that can take a photograph for facial recognition purposes, and then can switch the lens to capture an individual's iris image. For a facial photograph, the Agent will take a photograph approximately thirty (30) inches from a subject. Then, the Agent will switch the function of the device to capture iris. The Agent will then hold the device closer to the subject's eyes, ensure that the subject's eyes are open (and request that they open their eyes or not blink to ensure a high-quality image), and then click the device to collect an image of the subject's iris.

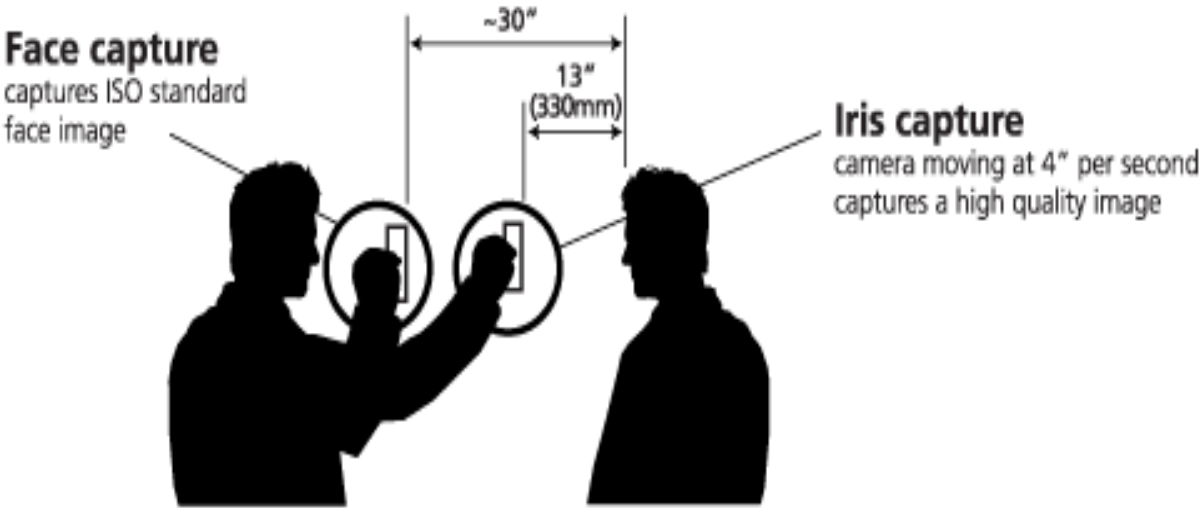

Figure 1: Difference in capture distance for facial photograph and iris scan.

All persons encountered by the U.S. Border Patrol attempting to enter the United States unlawfully, as well as those who are subject to removal, are subject to data collection requirements and processes (including providing biometric data). Currently, USBP collects ten (10) rolled fingerprints, iris scans, and facial photograph. These biometrics are searched and enrolled within the IDENT system and then the FBI's NGI system. These biometrics are also searched against the DOD ABIS database. Iris adds another type of multimodal biometrics for the best possible identification and verification using a combination of fingerprints, iris scans, and high-quality photographs. Following the success of the iris scan pilots from 2012, CBP has deployed iris scanning capabilities at some of the busiest Border Patrol Stations. CBP is actively deploying iris scanning cameras and mobile collection devices throughout the border environment.

e3 Detentions

The new e3 Detentions Module tracks certain information related to the location and movement of subjects during their period in CBP custody (via CBP Agent or Officer manual input, not using GPS or other tracking technology), generates lists for internal and external transfers of subjects, and allows CBP Agents to track and manage various custodial actions, such as meals, consular notifications, as well as, when appropriate, showers for adults and juveniles. Additionally, CBP can report certain information related to station cell conditions and the custodial care of all subjects in CBP custody. To support CBP operations, subject data is sent to the U.S. Department of Health and Human Services (HHS) Office of Refugee Resettlement (ORR) in order to provide placement/housing for families and juveniles in CBP custody. CBP sends information to HHS ORR electronically via encrypted email to eliminate previous duplicate data entry.

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 PIA in 2012. However, since the publication of the original e3 PIA, CBP has issued a new System of Records Notice (SORN) for records related to enforcement actions occurring between official ports of entry. The Border Patrol Enforcement Records (BPER) SORN[15] covers CBP's collection of information on individuals who it encounters, apprehends, detains, or removes in relation to border crossings, checkpoint operations, law enforcement actions, and other operations related to the enforcement of the Immigration and Nationality Act. This information may include biographic, biometric, and geolocation data, as well as enforcement-related information. The BPER SORN provides coverage for CBP's maintenance of records in e3.

e3 received its original Authority to Operate (ATO) on August 11, 2014. The e3 ATO is scheduled for renewal on August 12, 2017, pending completion of this PIA.

Characterization of the Information

e3 collects biographic and biometric data, encounter 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 e3 PIA.

In addition, CBP is expanding its collection of iris images to anyone encountered by the U.S. Border Patrol attempting to enter the United States unlawfully, as well as individuals who are subject to removal. Similar to fingerprints, CBP transmits iris data (in the form of a template) along with certain biographic data elements (including name, date and place of birth, and country of citizenship) to IDENT (and FBI NGI). IDENT performs a search against the data to identify whether the individual is associated with a previous encounter; the package is then enrolled and searchable for future queries. CBP will also retain the iris data in the subject's EID file. All applicable rules and memoranda of understanding (MOU) will continue to be followed including retention policies established by the host database SORN.

Privacy Risk: There is the risk that inaccurate information may be entered into the system.

Mitigation: Biometric data is collected directly from the individual and ensures that individuals are identified with a high degree of accuracy. In addition, CBP Border Patrol Agents are trained to employ interviewing and data entry techniques that reduce the risk of entering inaccurate information into the system. After a CBP Agent or Officer enters information in e3, the

[15] *See* DHS/CBP-023 Border Patrol Enforcement Records System of Records (BPER), 81 FR 72601 (October 20, 2016).

system also runs automatic and manual processes to ensure the integrity of the data, including scripts to check format and completeness and supervisory review.

Uses of the Information

Uses of the information within e3 have not changed since the original PIA publication. CBP continues to process biographic, biometric, encounter, and border-violence data through e3 for maintenance and retention in EID and IDENT. This information continues to be used to verify the unique identity of an individual in relation to an enforcement action. The iris image serves as an additional data point that CBP can use to verify the identity of an individual and evaluate information based on previous encounters.

The e3 Detentions Module allows CBP Border Patrol Agents to track the location and movement of subjects while in CBP custody and generates lists for internal and external transfers of subjects. For example, e3 Detentions generates the I-216 form, a manifest that tracks transfers of subjects between different facilities. The module also facilitates the management of various custodial actions (e.g., provision of meals, consular notifications, showers) and allows CBP to maintain the fitness of its facilities for safe custody.

The new Federal Person Query 2 Module facilitates the automatic retrieval of subject encounter data from multiple data systems using Web Services, and displays the consolidated data with biometric data within a single unified user interface. Prior to this function, CBP Border Patrol Agents conducted separate queries in the source systems; the new single unified interface builds the source system checks into the workflow and expedites the review of information while processing a subject without needing to log into other applications. This new federated query function does not pose any new privacy risks to data minimization or use limitation because users cannot query any systems to which they do not already have access. The access controls within e3 verify that CBP Border Patrol Agents have access to the underlying system or information before returning a query result. For instance, if an agent does not have valid access to NCIC or TECS information, he or she will not be able to view the information.

There are no new privacy risks regarding use of information in e3. All information is used for enforcement and border security actions.

Notice

All persons encountered by USBP attempting to enter the United States unlawfully, as well as those who are subject to removal, are subject to data collection requirements and processes that include providing biometric data. Individuals are made aware of the information collection requirements by signage posted at the ports of entry. Operational and logistical considerations prevent individuals encountered between ports of entry from receiving advanced notice of the data collection, but notice will be provided at the time the information is collected (during the

apprehension). All persons are provided general notice through this PIA and the newly issued BPER SORN,[16] the IDENT PIA,[17] and EID PIAs and SORN.[18]

Specifically regarding iris collection, individuals may be unaware that their iris is being collected during processing. However, Agents collect two different photographs from a subject during processing, at different distances from an individual's face. At the time of collection, Agents take a facial photograph, and then move the device closer to the subject, and request that the subject keeps his or her eyes open and does not blink. Agents do not explicitly tell subjects that the iris is being captured at the time of collection; however, this PIA provides notice of the process and procedure.

Due to the law enforcement nature of the encounter and purpose for collecting the information, CBP does not provide the opportunity for individuals to decline or consent to uses of information.

Privacy Risk: There is a risk that individuals may not realize that CBP is collecting their iris scans because the collection mechanism is the same as taking a photograph.

Mitigation: This risk is partially mitigated. Unlike collection of fingerprints, a subject does not have to make physical contact with an iris scanner for his or her information to be collected. While some iris scanning capabilities can collect iris scans from a distance, CBP has only deployed iris readers that require a subject to look into a high resolution camera for a special photograph. Individuals are positioned in front of the camera and aware that their picture is being taken for identification purposes. While they may not realize that their iris is being scanned concurrent with the capture of the photograph, typically at the time of collection, they are also being fingerprinted for identity verification. Due to the law enforcement nature of these collections, CBP may employ different types of biometric multimodal collections to determine the identity of the person encountered.

Data Retention by the Project

No changes have been made to data retention since the 2012 PIA; CBP will retain data in IDENT for 75 years, including iris images. CBP retains iris images in EID for three months in case of a transmission failure to IDENT, after which point they are destroyed.

[16] *See* DHS/CBP-023 Border Patrol Enforcement Records System of Records (BPER), 81 FR 72601 (October 20, 2016).
[17] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System, *available at* www.dhs.gov/privacy.
[18] *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID) and associated updates, *available at* www.dhs.gov/privacy, and DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 FR 72080 (October 19, 2016).

Internal Sharing and Disclosure

CBP data in EID is available to ICE Enforcement and Removal Operations (ICE ERO) and ICE Homeland Security Investigations (ICE HSI). ICE ERO requires access to this information when ICE ERO personnel take custody of subjects from USBP for removal, and ICE HSI uses the information for investigations.

In addition, CBP data in IDENT may be available to authorized users from the following DHS Components for the purposes listed below:

- CBP for screening travelers entering and exiting the United States and in support of identity verification during the course of border security enforcement and admissibility determinations;
- ICE for enforcement and investigative activities;
- U.S. Coast Guard for verifying crew members arriving in or accessing U.S. ports, and for enforcement activities related to sea interdictions;
- Transportation Security Administration for air exit initiatives and for issuing credentials to transportation and aviation workers (part of standard law enforcement and security checks);
- U.S. Citizenship and Immigration Services in order to process immigration, asylum, refugee, and other benefit applications, and background investigations for foreign adoptions;
- Federal Emergency Management Agency for issuing credentials to employees, local volunteers, and first responders;
- DHS National Protection and Programs Directorate for general enrollments of persons of interest for law enforcement and intelligence purposes, and for system administration (part of standard law enforcement and security checks); and
- DHS Office of the Chief Security Officer for employee background investigation purposes (part of standard law enforcement and security checks).

Privacy Risk: There is a risk that DHS Components may access CBP data in IDENT for activities that are inconsistent with CBP's original purpose for collecting the information.

Mitigation: This risk is partially mitigated. CBP, as a DHS Component, is permitted to share information within the Department as long as the recipient has a demonstrated need to know in the performance of his or her official duties. IDENT incorporates a filtering process based on CBP's requirements for information sharing. These filtering capabilities ensure that data is only shared with data provider-approved agencies for approved purposes. CBP has an interest in ensuring that information related to individuals it apprehends is broadly available to IDENT

partners for law enforcement, background investigation, and national security purposes. There remains some risk that information may be used beyond these activities; however, IDENT's auditing capabilities enable DHS to track who has accessed certain records and investigate any suspected use of information beyond the system's purpose.

External Sharing and Disclosure

The external sharing initiatives described in the 2012 PIA remain in effect. In addition and as described above, CBP may share subject information with HHS ORR to assist in refugee resettlement. CBP may also enroll biometric records along with the associated biographic data in FBI NGI as described above.

CBP information in IDENT may be available to the following agencies:

- the Department of State for processing visa applications, Border Crossing Card applications, general criminal history searches, and employee background investigations;
- To the Department of Justice, including the U.S. Marshals Service, the FBI, the Terrorist Screening Center, and the Bureau of Prisons for investigations, counterterrorism activities, and criminal history checks, including for state and local agencies;
- To the Department of Defense for biometrically enabled watchlisting, military operations as part of national security, and force protection searches;
- To the Office of Personnel Management Federal Investigative Service for employee and applicant background investigations;
- To the U.S. Office of Interpol for investigations related to international criminals, missing persons, and unknown deceased; and
- To international partners, including Germany (for limited law enforcement use) the United Kingdom (for visa issuance and biometric identity verification), and to Canada, New Zealand, and Australia (for biometric identity verification).

Privacy Risk: There is a risk that external users may access CBP data in IDENT for activities that are inconsistent with CBP's original purpose for collecting the information.

Mitigation: This risk is partially mitigated. IDENT incorporates a filtering process based on CBP's requirements for information sharing. These filtering capabilities ensure that data is only shared with data provider-approved agencies for approved purposes. CBP has an interest in ensuring that information related to individuals it apprehends is broadly available to IDENT partners for law enforcement, background investigation, and national security purposes. There remains some risk that information may be used beyond these activities; however, IDENT's auditing capabilities enable DHS to track who has accessed certain records and investigate any

suspected use of information beyond the system's purpose.

Privacy Risk: There is a potential privacy risk that external sharing could result in loss of control and the sharing of CBP biometric data without CBP's prior approval.

Mitigation: This risk is partially mitigated. There are controls in place to ensure that IDENT information is handled in accordance with the assigned user roles. External connections are documented and approved with each party's signature in Interconnection Service Agreements (ISA) that outlines controls in place to protect the confidentiality, integrity, and availability of information being shared or processed. Agencies with which IDENT shares information must agree to maintain reasonable physical, technical, and administrative safeguards to appropriately protect the shared information. Furthermore, recipient agencies must notify DHS as soon as reasonably practicable, but no later than 24 hours, after they become aware of any breach of security of interconnected systems or unauthorized use or disclosure of personal information. Disclosures outside of DHS must be accounted for in a paper or electronic record that includes the date, nature, purpose of each disclosure; and the name and address of the individual agency to which the disclosure is made.

Redress

The BPER SORN[19] asserts exemptions from the access provisions of the Privacy Act for the information maintained pursuant to their terms. Such exemptions are reviewed in the context of each request. To seek access to information collected through e3, individuals may request information about themselves, pursuant to the access provisions of the Privacy Act of 1974 (5 U.S.C. § 552a(d)) or pursuant to the Freedom of Information Act (FOIA) (5 U.S.C. § 552).

Any individual, regardless of citizenship or immigration status, may seek notification of and access to any CBP record contained in e3 pursuant to procedures provided by FOIA, and can do so by visiting https://www.cbp.gov/site-policy-notices/foia, or by mailing a request to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, DC 20229

When seeking records about one's self from any of the system of records applicable[20] or any other Departmental system of records, the request must conform to the Privacy Act regulations set forth in federal regulations regarding Domestic Security and Disclosure of Records and Information.

[19] *See* DHS/CBP-023 Border Patrol Enforcement Records System of Records (BPER), 81 FR 72601 (October 20, 2016).
[20] *See* DHS/CBP-023 Border Patrol Enforcement Records System of Records (BPER), 81 FR 72601 (October 20, 2016) and DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 FR 72080 (October 19, 2016).

The individual must first verify his or her identity, meaning that the requestor must provide his or her full name, current address, and date and place of birth. The requestor must sign his or her request, and the signature must either be notarized or submitted under federal statute regarding Unsworn Declarations Under Penalty of Perjury, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While an inquiry requires no specific form, forms may be obtained for this purpose from the DHS Chief Privacy Officer and DHS Chief FOIA Officer, https://www.dhs.gov/freedom-infomration-act-foia, or 1-866-431-0486. In addition, the request should:

- Explain why the requestor believes the Department would have information on him or her;
- Identify which component(s) of the Department the requestor believes may have the information about him or her;
- Specify when the requestor believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS Component agency may have responsive records.

If individuals are uncertain what agency or database manages the information, they may seek redress, regardless of citizenship, through the DHS Traveler Redress Program ("TRIP"), 601 South 12th Street, TSA- 901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip.

Privacy Risk: There is a risk that individuals are not aware of their ability to make record access requests for records in e3.

Mitigation: This risk is partially mitigated. This PIA and the BPER SORN describe how individuals may make access requests under FOIA or the Privacy Act. Redress is available for U.S. Citizens and Lawful Permanent Residents through requests made under the Privacy Act as described above. U.S. law prevents DHS from extending Privacy Act redress to individuals who are not U.S. Citizens, Lawful Permanent Residents, or the subject of covered records under the Judicial Redress Act. To ensure the accuracy of CBP's records, CBP may permit access and amendment, regardless of citizenship, on a case-by-case basis, consistent with law.

In addition, providing individual access or correction of e3 records may be limited for law enforcement reasons as expressly permitted by the Privacy Act. Permitting access to the records contained in e3, regardless of a subject's citizenship, could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, or to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

Privacy Risk: There is a risk that individuals may file a Privacy Act request with CBP with regard to access, correction, or amendment to their biometric data and CBP will be unable to fix the underlying biometric information since OBIM, as the biometrics service provider for the Department, maintains the physical repository of the data.

Mitigation: This risk is partially mitigated. Individuals, regardless of citizenship, may 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 TRIP
601 South 12th Street
TSA-901
Arlington, VA 20598-6901

Completing the form online saves processing time and helps prevent data entry errors. After an individual submits a redress form, the individual will receive notification of receipt from DHS TRIP. DHS TRIP will review the redress form and will determine which component/agency will be able to respond most effectively to the redress request. When a redress request is related to a CBP e3 event, DHS TRIP will coordinate with CBP. CBP will then review the individual's records and correct the information, if appropriate. DHS TRIP will notify the individual of the resolution of that request. If an individual is dissatisfied with the response to his or her redress inquiry, then he or she 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, Department of Homeland Security, Mailstop 0655, 245 Murray Lane, Washington, D.C. 20528, USA; or by fax: 1-202-343-4010. As with access, amendments may be limited pursuant to exemptions asserted under 5 U.S.C. § 552a (j)(2) and (k)(2) for the IDENT system.

Privacy Risk: Due to the law enforcement nature of the information within e3, there is a risk that individuals will not be able to access, correct, or amend their records since the records are exempted from access, correction, and amendment under the Privacy Act.

Mitigation: This risk is partially mitigated. Information from certain CBP source systems may be amended as indicated in the applicable SORN. However, providing individual access or correction of e3 records may be limited for law enforcement reasons, including as expressly permitted by the Privacy Act. Permitting access to the records contained in e3 could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, or to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

Privacy Risk: With the recent cancellation of the DHS Mixed Systems policy[21] through DHS Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information*,[22] there is a risk that non-U.S. Citizens and non-Lawful Permanent Residents are now unable to access, correct, and amend their information as they were previously able to do.

Mitigation: This risk is partially mitigated. This PIA and source system SORNs describe how individuals can request access under FOIA or the Privacy Act. Redress is available for U.S. Citizens and Lawful Permanent Residents through requests made under the Privacy Act as described above. U.S. law prevents DHS from extending Privacy Act redress to individuals who are not U.S. Citizens, Lawful Permanent Residents, or the subject of covered records under the Judicial Redress Act. However, these individuals still may seek notification of and access to records pursuant to procedures provided by FOIA. Additionally, to ensure the accuracy of CBP's records, CBP may permit access and amendment, regardless of citizenship, on a case-by-case basis, consistent with law.

Auditing and Accountability

All e3 users undergo initial security awareness training, and thereafter complete the DHS online security awareness-training course annually. The CBP Security and Technology Policy Branch provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and annually thereafter as refresher training. CBP requires by policy that all information system users (including managers, senior executives, and contractors) participate in the provided training within 24 hours of being granted a user account and at least annually thereafter. This policy adheres to DHS security awareness training policies. To ensure all CBP employees participate in the security awareness training, there are emails distributed as well as reminders posted to the CBP intranet. Additionally, a memorandum from the Assistant Commissioner, Office of Information Technology, is distributed to all CBP employees via the CBP intranet. The memorandum reiterates that access to the CBP network will be disabled if training is not completed, and that the DHS Office of Inspector General audits training records to verify compliance. Participation in the security awareness training is tracked, monitored, and reported to the Office of Information Technology (OIT) to ensure compliance with DHS and CBP security awareness training polices.

The e3 application access control procedures adhere strictly to the DHS Sensitive Systems

[21] For more information, please *see* Privacy Policy Guidance Memorandum 2007-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons, available at* https://www.dhs.gov/privacy.
[22] For more information about the recent cancellation of the DHS Mixed Systems policy, please *see* the DHS Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information, available at* https://www.dhs.gov/privacy.

Policy Directive 4300A and CBP Information System Security Policies and Procedures Handbook 1400-05D. Every authorized e3 application user, after completing a favorable background investigation is issued a unique Hash ID and password to gain access.

All MOUs and Interconnection Service Agreements (ISA), including those related to e3, are created by the e3 administrators. MOUs for the e3 portal are sent to the CBP Privacy Officer for review and to DHS for final approval.

All connections are documented via a memo or elaborated upon within the e3 Security Plan (SP). All connections are monitored, and documents such as the ISA and SP are regularly updated. Whenever a major change to any connection occurs then the ISA must be reviewed and revised, if necessary. If there is a need for a new ISA then a new ISA will be completed and approved. The ISAs must be approved by the designated Authorizing Official.

Privacy Risk: There is a privacy risk that CBP does not have control over the security, auditing, and accountability of IDENT users who may access and share CBP biometrics, and how OBIM may be sharing IDENT data.

Mitigation: This risk is partially mitigated. OBIM/IDENT secures its data by complying with the requirements of DHS information technology security policy, particularly the DHS Information Technology (IT) Security Program Handbook for Sensitive Systems (Attachment A to DHS Management Directive 4300.1). This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules. IDENT is periodically evaluated to ensure that it complies with these security requirements.

IDENT also provides audit trail capabilities in order to monitor, log, and analyze system transactions, as well as actions and system accesses of authorized IDENT users.

Because IDENT contains data from a variety of sources, collected for a variety of uses, it is necessary to institute controls so that only those individuals with a need to know are able to access that data. IDENT has a robust set of access controls, including role-based access and interfaces, which limit individual access to the appropriate discrete data collections. Misuse of the data in IDENT is mitigated by requiring that IDENT 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 by both parties through a signed ISA that outlines the controls in place to protect the confidentiality, integrity, and availability of the information being shared or processed.

Users of the IDENT system, and all employees and contractors supporting IDENT, have limited access based on their roles and need to know. Users are trained in the handling of PII. All

IDENT users must complete annual refresher training to retain system access.

OBIM has documented standard operating procedures to determine which users may access the IDENT system. The minimum requirements for access to the IDENT system is documented in the MOU/data-sharing agreement between OBIM and CBP, and in security, technical, and business documentation. In particular, individuals with system access must hold a DHS security clearance, must have a need to know the information based on their job responsibilities, and must participate in security and privacy training. Also, IDENT data-filtering rules enable role-based access to information within IDENT pursuant to access rules provided by the data provider.

Contract personnel may additionally have access to IDENT data. The extent of access will vary, based on the need to fulfill the requirements of the contract under appropriate nondisclosure and use limitations, and subject to requirements enumerated in Section 8.1 of the original e3 PIA. OBIM ensures that all employees and contractors supporting its systems have limited access based on their roles and that they are trained in the handling of PII.

Responsible Official

Antonio J. Trindade
U.S. Border Patrol
U.S. Customs and Border Protection
Department of Homeland Security

Debra L. Danisek,
CBP Privacy Officer
U.S. Customs and Border Protection
Department of Homeland Security

Approval Signature

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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security