



Privacy Impact Assessment
for the

CBP Portal (E3) to ENFORCE/IDENT

DHS/CBP/PIA-012

July 25, 2012

ContactPoint

Antonio J. Trindade

**U.S. Customs and Border Protection
Border Enforcement and Investigations Systems
(202) 344-1446**

Reviewing Official

Mary Ellen Callahan

Chief Privacy Officer

**Department of Homeland Security
privacy@dhs.gov**



Abstract

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) has established E3, the CBP portal to U.S. Immigration and Customs Enforcement's (ICE) Immigration and Enforcement Operational Records System (ENFORCE), Enforcement Integrated Database (EID),¹ and US-VISIT's Automated Biometric Identification System (IDENT),² to collect and transmit data related to law enforcement activities. E3 collects and transmits biographic, encounter, and biometric data including, but not limited to, fingerprints for identification and verification of individuals encountered at the border for CBP's law enforcement and immigration mission.

In addition to the collection of fingerprints, beginning at the end of July 2012, the E3 portal will begin a six-week pilot program to collect iris scans of individuals apprehended by CBP Border Patrol at the McAllen, Texas, Border Patrol Station. Collection of iris scans provides the capability to capture biometric data from individuals if their fingerprints cannot be obtained, and also to biometrically compare and authenticate an individual's identity. In different operational environments, Iris scans can be captured more quickly than fingerprints, are as or more reliable in providing a unique biometric, do not involve the touching of the subject, with respect to those cultures for whom such contact poses a concern, and require less storage capacity and transmission bandwidth than fingerprints. This privacy impact assessment is being conducted because E3 requires the collection of personally identifiable information (PII).

Overview

The Department of Homeland Security, U.S. Customs and Border Protection E3 portal consists of a series of web applications that collect and transmit collected data to ICE's ENFORCE-EID and US-VISIT's IDENT databases for processing, identification, and verification of violators encountered at the border. E3 is a transactional interface and does not store the collected data. Rather, E3 is used as a portal to transmit data in real-time from Border Patrol (BP) Agents and CBP Officers to the respective databases and retrieve records for CBP enforcement purposes. BP Agents and CBP Officers collect PII from the public as part of the apprehensions workflow, which includes interviewing the subject and collecting biographic and biometric data; recording any related incidents of border violence; recording data concerning seized property in relation to an apprehension; and prosecuting the subject. Also, BP Agents and CBP Officers may cross reference CBP TECS and E3 and make notations in their narratives in the Processing and Prosecutions Modules (discussed below) of the relevant TECS record or

¹ DHS/ICE/PIA-015 Enforcement Integrated Database (EID) and associated updates and DHS/ICE-011 Immigration Enforcement Operational Records System of Records (ENFORCE) published May 3, 2010 (75 Fed. Reg. 23274).

² DHS/USVISIT/PIA-002 US VISIT IDENT and associated updates and DHS/USVISIT-012 DHS Automated Biometric Identification System (IDENT) June 5, 2007 (72 Fed. Reg. 31080).



ENFORCE-EID Record. BP Agents and CBP Officers must log into a separate account to access and record information in TECS, which is covered by a separate PIA.³

The E3 portal consists of the following modules:

- **Processing Module:** The E3 Processing Module allows CBP Officers and BP Agents to record an apprehended individual's biographic information as well as seized property.
- **Biometrics Module:** The Biometric Module provides the E3 interface to the US-VISIT IDENT service.⁴ The Biometrics Module allows BP Agents and Officers to 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. IDENT searches for possible matches among the repository of fingerprint images in the database. Query results are returned to the E3 Biometric Module. IDENT either matches the fingerprint image to a previously encountered individual's scanned fingerprint or enrolls the fingerprint image in its database by assigning a Fingerprint Identification Number (FIN) since the individual had no biometric records stored in any of the databases. IDENT is the sole repository for the fingerprint image, but the FIN is sent back to the E3 Biometric Module along with any biographic information associated with that fingerprint. The CBP Officer or BP Agent would then compare the query results with the previous encounter records, and look at recidivism to determine if the subject meets a threshold set for a particular enforcement action.

In addition to the collection of fingerprints, beginning at the end of July 2012, the E3 portal will begin a six week limited production pilot program to collect iris scans from all individuals apprehended by CBP Border Patrol at the McAllen, Texas, Border Patrol Station. Upon conclusion of the pilot, CBP will suspend its collection of iris scans to assess the operational deployment of the iris scanning technology. Collection of iris scans provides the capability to capture a higher quality and more consistent biometric identifier for individuals. The captured iris scan will be transmitted in real-time to IDENT to query for a possible match, going forward, and the iris scans will be retained in IDENT. An individual will have one FIN assigned for both iris scans and fingerprints from each encounter to ensure there is only one identifier per person. If a previously-encountered individual is found, IDENT will match up the multiple biometrics to one FIN. The

³ DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Screening and associated updates and DHS/CBP-011 CBP TECS published December 19, 2008 (73 Fed. Reg. 77778).

⁴System of Records Notice (SORN) at [DHS/USVISIT-0012 - DHS Automated Biometric Identification System \(IDENT\)](#) June 5, 2007, 72 FR. 31080



FIN will be used to uniquely identify individuals and to link and retrieve immigration and border management records with a single identifier instead of multiple identifiers. The collection of iris scans will enhance CBP's ability to identify those who present threats and facilitate the appropriate enforcement action for those who CBP Border Patrol has encountered and checked before.

- **Assault Module:** The Assault Module provides a web-based interface to facilitate the capture and recording of data pertaining to border violence. BP agents make entries to the Assault Module if an incident involved an assault on a BP Agent. Data entries include: type of weapon used in the incident; name of the agent assaulted; time/date of the incident; location of the incident; and the agent's current duty location.
- **Prosecutions Module:** The Prosecutions Module provides a web-based interface allowing BP Agents to view and record information pertaining to criminal trials. The Prosecution Module is integrated with the Processing and Biometric Modules allowing BP Agents to enter, acquire, update, and track data pertaining to investigations and criminal prosecutions. The Prosecutions Module allows BP Agents to create prosecution cases, electronic case file and print cases, update and track cases, and create statistical reports. CBP, through a memorandum of understanding (MOU) between DHS and the Department of Justice (DOJ), is required to upload data from the Prosecutions Module via a secure connection to a DOJ web site to facilitate criminal prosecutions and also provide material witness affidavits. The DOJ web site is accessible by authorized court officials but not directly available to the public.
- **Operations Against Smugglers Initiative on Safety and Security (OASISS) Module:** The OASISS Module tracks and manages OASISS cases and helps facilitate the prosecution of alien smugglers and human traffickers who operate in border communities. Additionally, by keeping track of case information associated with alien smugglers, it will help maintain continuity within the case and aid in future U.S. Alien Smuggling and OASISS cases.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The data entered into the E3 Modules is collected based on the authorities specified in 6 U.S.C. § 202; 8 U.S.C. §§ 1103, 1158, 1201, 1225, 1324, 1357, 1360, 1365a, 1365b, 1379, and 1732; 19 U.S.C. §§ 2071, 1581-1583 and 1461.



1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The E3 portal is covered under the following SORNs: DHS/ICE-011 - Immigration and Enforcement Operational Records System (ENFORCE) May 3, 2010, 75 FR 23274 and DHS/USVISIT-0012 - DHS Automated Biometric Identification System (IDENT) June 5, 2007, 72 FR 31080. Encounters are transmitted to, and maintained in ENFORCE. Biometric scans and associated biographic information collected by CBP Officers and BP Agents are transmitted to, and stored in, the IDENT system.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. E3 was granted an Authority to Operate (ATO) on August 9, 2011.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. The retention schedule for IDENT and for EID have been approved by NARA.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Information stored in US-VISIT (IDENT) is covered under OMB collection number 1600-0006. No other information collected during the encounter is subject to the PRA because it is a law enforcement encounter.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The information that the E3 portal collects and transmits to ENFORCE-EID and IDENT includes biographic, biometric, encounter, border violence, and prosecution-related data obtained from individuals during encounters in operation/production, testing, and training environments. The information listed below is not exhaustive; other data may be collected that is consistent with the general categories listed below.



1. Biographic data includes:

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

2. Biometric data includes:

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

3. 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: U.S. CIS Benefit Number; State ID number; Alien File Number; Travel Document Number
- Fingerprint Identification Number (FIN)
- Violations



4. Border violence data includes:
 - Name of Agent
 - Assailant's Information
 - Injury descriptions
 - Hospital names and locations
 - Witness accounts and information
 - Weapon descriptions
5. Prosecutions data includes:
 - Charges
 - Case dates
 - Verdicts
 - Subject information
 - Attorney information
 - Judge information
 - Sentencing information
 - Release dates

2.2 What are the sources of the information and how is the information collected for the project?

E3 applications use data collected from individuals during an encounter, including information collected using fingerprint, iris, and bar code scanners. E3 uses data from law enforcement databases including, IDENT and ENFORCE. Also, BP Agents and CBP Officers may cross reference TECS and E3 and make notations in their narratives in the Processing and Prosecutions Modules of the relevant TECS record or ENFORCE-EID Record. Users enter information using a common user interface.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No, E3 does not use data from commercial or public source providers.



2.4 Discuss how accuracy of the data is ensured.

There are numerous data quality checks built into E3 to ensure accuracy of the data collected. These quality checks include client-side and server-side scripts, which check to ensure required fields are not blank and data is entered in the correct format. In addition, the E3 system is encrypted with rules to check for data accuracy. Also, E3 is equipped with a mapping functionality that automatically provides geographic (latitude/longitude) information associated with an encounter. At the end of each shift, supervisors review information that agents enter into the E3 system.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

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

Mitigation: The training and interviewing techniques employed by CBP Officers and the BP Agents, reduce the risk of inaccurate information being entered in the system. Once data are entered into the system, automatic and manual processes are in place to ensure the integrity of the data, including scripts to check format and completeness and supervisory review.

Privacy Risk: Results from IDENT may inaccurately identify an individual or inaccurately match an individual to derogatory data.

Mitigation: To mitigate the risk of an inaccurate match, US-VISIT's Biometric Support Center employs highly trained forensic analysts to verify biometrics where a question arises. CBP Officers and BP Agents alert US-VISIT where inaccuracies are found to prevent further mismatches.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

Data accessed through E3, including biographic, biometric, encounter, and border-violence data maintained in ENFORCE-EID and IDENT are used to verify the unique identity of an individual within the immigration and border management enterprise.

The E3 Processing Module is designed to support the law enforcement arrest and booking functions of CBP, including apprehension processing, fingerprint and photographic identification, recording of allegations and charges, preparation and printing of appropriate forms, and interfaces with other applications. This module allows CBP to track the apprehension



of individuals (both non-U.S. Citizens and U.S. Citizens) who have been arrested by CBP for violating U.S. customs and other laws, including provisions of the Immigration and Nationality Act (Title 8, United States Code).

The Biometrics Module allows CBP Officers and BP Agents to uniquely identify or verify the identity of the individuals they encounter by transmitting biographic and biometric data to IDENT.

The E3 Assault Module provides a web-based interface for BP agents to record assault data. The E3 Prosecution Module integrates with E3 Processing and E3 Biometrics event data. This allows BP agents to enter, acquire, update, and track data pertaining to allegations and criminal prosecution. BP agents can create prosecution cases, e-file and print cases, update and track cases, and create statistical reports.

The OASISS Module tracks and manages OASISS cases and helps facilitate the prosecution of alien smugglers and human traffickers who operate in border communities. Additionally, by keeping track of case information associated with alien smugglers, it will help maintain continuity within the case and aid in future U.S. alien smuggling and OASISS cases.

During the pilot program, CBP will collect iris scans for submission to IDENT to evaluate how well this new collection provides for identity verification and whether it is easily cross-referenced with the fingerprints and biometric information on file. It is anticipated the pilot will demonstrate that iris scan may be obtained more quickly, are as or a more reliable biometric than fingerprints, and require less storage capacity and transmission bandwidth than fingerprints. Additionally, it is expected to be met with less resistance by subjects because the collection does not require any touching, which is both culturally sensitive and reduces maintenance and interaction required by BP Agent.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. E3 does not discover or locate a predictive pattern or anomaly indicative of criminal behavior. E3 captures information to be transmitted to the ENFORCE-EID or IDENT systems. When a biometric (fingerprint and/or iris scan) of an individual is submitted to US-VISIT to conduct a query, IDENT searches for a match among the retained images. Query results are returned to the E3 Biometric application. The E3 Processing Module has the capability to perform subject searches using identifiers such as A-Number, last name, or FIN. CBP Officers and BP Agents are able to conduct queries through E3 against the repository systems for identity



verification and cross-checking but the E3 modules – Processing, Biometrics, Assault, Prosecutions, and OASISS – are not used to data mine information from these systems.

3.3 Are there other components with assigned roles and responsibilities within the system?

The biometric data (fingerprints and iris scans) and encounter information provided to US-VISIT for matching can be accessed by other DHS components, including ICE, United States Citizenship and Immigration Services (USCIS), and CBP on a need-to-know basis. However, only CBP officers and BP Agents have the ability to edit CBP information through the E3 portal.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Risk: The potential privacy risks include unauthorized access and use and disclosure of the data/information.

Mitigation: There are controls in place to ensure that information is handled in accordance with the assigned user roles. All CBP employees, contractors, and any other authorized personnel having access to the E3 portal are required to take a mandatory IT Security Awareness Training through the online Virtual Learning Center (VLC). The training provides instructions on the use and handling of sensitive information, including PII. In addition, access to E3 is limited through specific roles and periodic audits. E3 uses role-based profiles (standard user and privileged user) that enforce Discretionary Access Control Lists (DACL)'s to prevent unauthorized access to different levels of data within each module and provides an additional layer of protection from unauthorized alteration, loss, unavailability, or disclosure of information.

Risk: There is a privacy risk that the iris scan will be incorrectly cross-referenced with fingerprints.

Mitigation: The BP agents who will be operating the iris scanning technology have received training regarding in the use of both the iris scanners and the fingerprint readers. This training ensures that the BP agent will only assign one identification number to both biometrics, and that the agent will confirm the biographic information from the subject as part of the assignment of the identification number. Lastly, US-VISIT IDENT provides redress for persons who allege that their biometrics are misidentified.



Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

All persons entering the United States are subject to data collection requirements and processes including providing biometric data. Individuals are made aware of the information collection requirements by signage posting at the points of entry (POEs). Individuals encountered between ports of entry may not be provided advanced notice, but will be provided notice at the time the information is collected (during the apprehension). All persons are provided general notice through this PIA and the EID and IDENT PIAs and SORNs.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Due to the law enforcement nature of the encounter and purpose for collecting the information, including the iris scans collected during the pilot program, the collection of iris scans will be mandatory for individuals encountered in the station in which the pilot is conducted. CBP does not provide the opportunity for individuals to decline to provide or consent to uses of information.

4.3 Privacy Impact Analysis: Related to Notice

Risk: CBP may collect information from individuals without providing notice or without the consent of the individual.

Mitigation: While individuals encountered between ports of entry may not be provided advanced notice, they will be provided notice at the time the information is collected (during the apprehension). Additionally, all persons are provided general notice through the publication of this PIA and the publication of the EID and IDENT PIAs and SORNs on the DHS web site. Personnel with access to information must complete a full field background investigation and complete privacy training to mitigate against the misuse of this data.



Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

The information collected through E3 including the iris scans during the pilot is transmitted in real time to US-VIST/IDENT for identity verification and is retained in the US-VISIT database. In addition, E3 transmits the encounter or case information, including biographic information about the subject, nature of the violation, and any narrative report by the BP agent, to ENFORCE for processing of the alleged violation. In accordance with the IDENT and ENFORCE SORNs, records associated with E3 will be retained until the statute of limitations has expired for all violations or until the records are older than 75 years, whichever is longer.

5.2 Privacy Impact Analysis: Related to Retention

Risk: There is the risk that PII may be retained in the system for a longer period than is necessary for the purpose for which the information was collected.

Mitigation: The records retention periods approved for IDENT and EID as related to E3 are appropriate and consistent with CBP's immigration and law enforcement missions.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

CBP officers and BP Agents, through an MOU between DHS and DOJ, upload data from the Prosecutions Module via a secure connection to the DOJ website to facilitate criminal prosecutions and also provide material witness affidavits. The DOJ web site is accessible by authorized court officials but not available to the public.

Information may be shared with the appropriate federal, state, local, tribal, and foreign government agencies or multi-lateral governmental organizations responsible for investigating or prosecuting the violations of law, to support the enforcement of border security and immigration laws. Sharing will occur in accordance with the provisions of the Privacy Act (5 U.S.C. § 552a) and the routine uses listed in the ENFORCE and IDENT SORNs.



However, iris scans collected during the pilot program will not be shared outside DHS unless required by law.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

All external disclosures to federal, state, local, foreign, and private entities of information obtained through the E3 portal and maintained in either IDENT or ENFORCE will be in strict compliance with the routines uses of the respective SORN.

E3 information may be disclosed pursuant to the routine uses outlined in the IDENT or ENFORCE SORNs, as appropriate.

6.3 Does the project place limitations on re-dissemination?

Yes. Prior to each sharing of information with a federal, state, or local agency, an MOU or other written authorization places limitation on the use and re-dissemination.

CBP officers and BP Agents using the E3 Prosecutions Module upload data via a secure DOJ website. All CBP Officers and BP Agents using the DOJ website must have a user name and password issued by DOJ.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Disclosures outside of DHS must be accounted for in a paper or electronic record which includes the date, nature, purpose of each disclosure; and the name and address of the individual agency to which disclosure is made. *Ad hoc* requests must be approved by the appropriate Program Director, and filed.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: The primary risk of sharing data with an external agency or government is interception of the data or misuse of the data by an employee.

Mitigation: For the Prosecutions Module, these risks are mitigated by DOJ secure website and authentication of DHS employees to the DOJ system. With respect to information shared through facilitated access, the risk of interception is mitigated through confirmation of email address or fax number for the requestor prior to transmission of the responsive records.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.



7.1 What are the procedures that allow individuals to access their information?

Both IDENT and ENFORCE SORNs, assert 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). Individuals may seek access to their specific information by filing a FOIA or Privacy Act request in writing, including a daytime phone number and email address. Individuals should provide as much information as possible on the subject matter to expedite the search process. Requests should be sent to:

U.S. Customs and Border Protection
FOIA Division
799 9th Street NW, Mint Annex
Washington, DC 20229-1181
Telephone: (202) 325-0150.

More information is available at http://www.cbp.gov/xp/cgov/admin/fl/foia/reference_guide.xml.

Individuals can submit a Freedom of Information Act (FOIA) request using procedures outlined on the CBP web page at:

http://www.cbp.gov/xp/cgov/admin/fl/foia/making_a_request/reference_guide.xml

Individuals may contest information collected through E3 or in ENFORCE/IDENT in the context of any immigration or criminal proceedings that result from the encounter.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals may seek access to their specific information by filing a Freedom of Information Act or Privacy Act request. Also, individuals may contest information collected through E3 and maintained in ENFORCE/IDENT through any immigration or criminal proceedings that result from the encounter. CBP has a FOIA Office to provide redress with respect to incorrect or inaccurate information collected or maintained by its electronic systems or other electronic systems in which CBP records are maintained. Inquiries should be directed to the FOIA Office at:



U.S. Customs and Border Protection
1300 Pennsylvania Ave., NW
Attn: Mint Annex Building, FOIA Division
Washington, D.C. 20229
Telephone: (202) 325-0150

7.3 How does the project notify individuals about the procedures for correcting their information?

CBP has a FOIA Office to provide redress with respect to incorrect or inaccurate information collected or maintained by its electronic systems or other electronic systems in which CBP records are maintained. Inquiries should be directed to the FOIA Office at:

U.S. Customs and Border Protection
1300 Pennsylvania Ave., NW
Attn: Mint Annex Building, FOIA Division
Washington, D.C. 20229
Telephone: (202) 325-0150

7.4 Privacy Impact Analysis: Related to Redress

Risk: Individuals may suffer negative effects as a result of the data used by E3 without the ability to correct it.

Mitigation: Information can be corrected as appropriate by authorized CBP employees as additional information is gathered or updates provided to the CBP Officer or BP Agent through proceedings and/or interviews. Further, information collected or used by E3 may be contested through the immigration or criminal proceedings that may result from the encounter.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

E3 has a robust set of access controls including role-based access and interfaces which limit individuals' access to the data to which they should have access. These include the ability of certain users to apply *ad hoc* security restrictions to particular records. Misuse of data collected by and accessed through E3 is prevented or mitigated by maintaining audit trails – including, at a minimum, user name, access date and time, and functions and records addressed – and by requiring that users conform to appropriate security and privacy policies, follow established rules of behavior, and be adequately trained regarding the security of the system.



Also, a periodic assessment of physical, technical, and administrative controls is performed to enhance accountability and data integrity.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All E3 users undergo initial security awareness training, and thereafter complete the DHS online security awareness-training course annually.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Active Directory, Mainframe, and Border Patrol Enforcement Tracking System (BPETS) Teams handle the account creation for the Processing, Biometrics and Prosecutions Modules. Agents obtain a role in each module by requesting and obtaining supervisor and module administrator approval. The Assault Module relies on a Password Issuance and Control System (PICS) ID for authentication, in addition to supervisor approval. Users are granted access to OASISS only when the OASISS coordinator for the agency makes a request on behalf of the user.



8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All memoranda of understanding (MOUs) and Interconnection Service Agreements (ISAs), including those related to E3, are created by the E3 administrators. MOUs and ISAs for the E3 system are sent to the CBP Privacy Officer for review and to DHS for final approval.

Responsible Officials

Laurence Castelli
CBP Privacy Officer
U.S. Customs and Border Protection
(202) 325-0280

Antonio J. Trindade
Associate Chief, Enforcement Systems
Office of Border Patrol
U.S. Customs and Border Protection
(202) 344-2619

Approval Signature

Original signed and on file with the DHS Privacy Office.

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security