Privacy Impact Assessment

for the

Unified Immigration Portal (UIP)

DHS Reference No. DHS/CBP/PIA-072

April 1, 2022

Homeland Security

Abstract

The U.S. immigration system is complex, involving multiple federal government stakeholders, processes, and information technology systems. This complexity creates challenges between agencies involved in the immigration process that need to share and receive comprehensive, consistent, and timely information required to make impactful and mission-critical decisions. The U.S. Customs and Border Protection (CBP) Unified Immigration Portal (UIP) provides agencies involved in the immigration process a means to view and access certain information from each of the respective agencies from a single portal in near real time (as the information is entered into the source systems). CBP is publishing this Privacy Impact Assessment (PIA) to provide notice of implementation of the UIP and assess the privacy risks and mitigations for the UIP.

Overview

The United States immigration system requires coordination between multiple U.S. federal governments agencies, each responsible for administering different aspects of the U.S. immigration system. The Department of Homeland Security (DHS) has three components with immigration enforcement and benefits responsibilities: 1) CBP is responsible for border security and border enforcement, and for the inspection and initial processing of noncitizens at the border; 2) U.S. Citizenship and Immigration Services (USCIS) adjudicates immigration-related benefits and requests; and 3) U.S. Immigration and Customs Enforcement (ICE) performs immigration enforcement functions throughout the Nation. In addition to DHS, the Department of Justice (DOJ) Executive Office for Immigration Review (EOIR) administers immigration court proceedings, while the Department of Health and Human Services (HHS) Office of Refugee Resettlement (ORR) provides certain eligible populations with critical resources, and provides for the placement of certain migrant populations, in particular, unaccompanied noncitizen children.[1]

The aforementioned agencies each have a unique mission with their own authorities, processes, stakeholders, and information technology systems. This complexity has sometimes made it difficult for agencies involved in the immigration process to quickly and easily receive and visualize the comprehensive, consistent, and timely information required to make impactful and mission-critical decisions. For example, in some instances, because individual government agencies rely on disparate data sources, sharing information between agencies for operational awareness sometimes requires each agency to manually pre-process and format data to meet the

[1] There are other agencies such as the Department of State (DOS) who play a key role in the immigration process as well. However, the role and contributions of those agencies are out of scope of this Privacy Impact Assessment. CBP will update this Privacy Impact Assessment, should additional agencies become involved in this information sharing initiative.

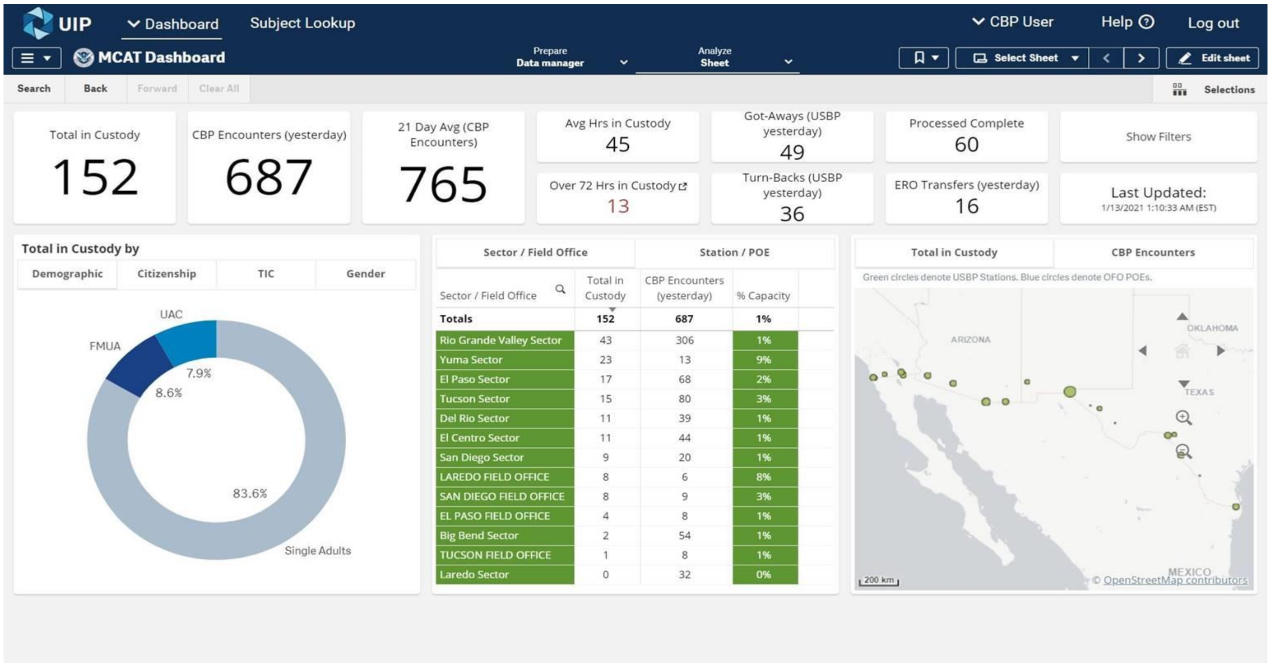
needs of the receiving agency for both operational awareness and statistical analysis. Manual pre-processing of data elements from multiple stakeholder agency data sources requires a significant amount of time and labor resources and involves a higher possibility of data entry errors.

Following the surge at the U.S. Southwest border in Summer 2019, federal agencies identified the need to address challenges posed by a lack of information-sharing within the U.S. immigration system. In response, DHS conceived the Unified Immigration Portal (UIP) as an interagency solution between CBP, USCIS, ICE, DOJ, and HHS. The UIP was developed to connect relevant data from agencies across the immigration lifecycle to enable a more complete understanding of an individual's immigration journey.

To provide real-time statistics and more efficient access to key immigration data between agencies, CBP developed the UIP to visualize data sets already accessed by government immigration stakeholders. The UIP is an integrated solution for immigration data visualization and reporting, which provides visibility of complete and near real-time information across multiple agencies involved in the immigration process. The UIP is designed to enable users to more easily view, use, and access data across multiple federal government stakeholder agencies while accounting for differing role-based access levels and data protection requirements across the various users from each stakeholder agency.

The UIP allows each agency involved in the immigration process to share certain data[2] from their respective agency's immigration information technology systems through the UIP portal. The UIP aggregates the disparate data sources, links related data elements, and visualizes those data elements in one location using dashboards. For example, as shown below, the dashboard view serves as the landing page for users accessing the UIP and displays near real-time priority information such as in-custody metrics, encounters, and transfers.

[2] UIP temporarily displays data without storage. The UIP displays information in near real-time. As the information is updated in the source system, it will be available for display in the UIP. The refresh rate is roughly every 30 minutes.



Total in Custody 152

CBP Encounters (yesterday) 687

21 Day Avg (CBP Encounters) 765

Avg Hrs in Custody 45

Over 72 Hrs in Custody 13

Got-Aways (USBP yesterday) 49

Turn-Backs (USBP yesterday) 36

Processed Complete 60

ERO Transfers (yesterday) 16

Last Updated: 1/13/2021 1:10:33 AM (EST)

Total in Custody by

Demographic | Citizenship | TIC | Gender

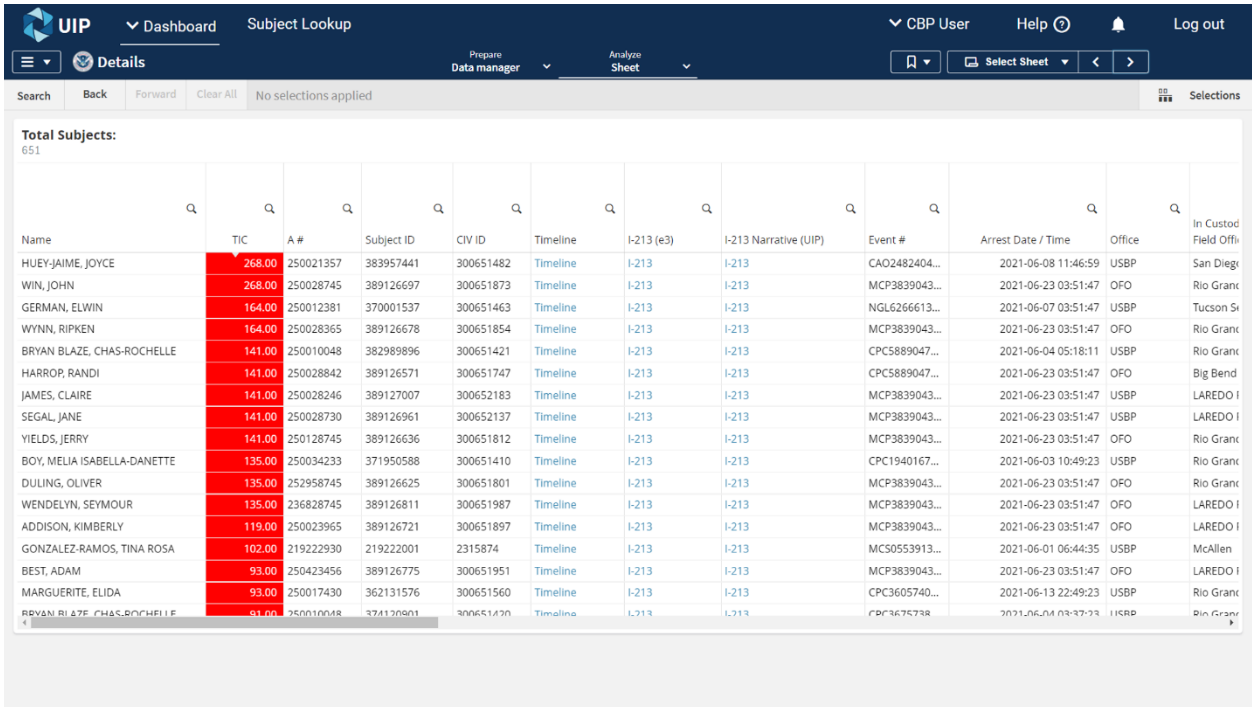
Sector / Field Office | Station / POE

Sector / Field Office	Total in Custody	CBP Encounters (yesterday)	% Capacity
Totals	152	687	1%
Rio Grande Valley Sector	43	306	1%
Yuma Sector	23	13	9%
El Paso Sector	17	68	2%
Tucson Sector	15	80	3%
Del Rio Sector	11	39	1%
El Centro Sector	11	44	1%
San Diego Sector	9	20	1%
LAREDO FIELD OFFICE	8	6	8%
SAN DIEGO FIELD OFFICE	8	9	3%
EL PASO FIELD OFFICE	4	8	1%
Big Bend Sector	2	54	1%
TUCSON FIELD OFFICE	1	8	1%
Laredo Sector	0	32	0%

Total in Custody | CBP Encounters

Green circles denote USBP Stations. Blue circles denote OFO POEs.

Figure One: UIP Apprehension Dashboard (mock data only)



No selections applied

Total Subjects:
651

Name	TIC	A #	Subject ID	CIV ID	Timeline	I-213 (e3)	I-213 Narrative (UIP)	Event #	Arrest Date / Time	Office	In Custod Field Offi
HUEY-JAIME, JOYCE	268.00	250021357	383957441	300651482	Timeline	I-213	I-213	CAO2482404...	2021-06-08 11:46:59	USBP	San Dieg
WIN, JOHN	268.00	250028745	389126697	300651873	Timeline	I-213	I-213	MCP3839043...	2021-06-23 03:51:47	OFO	Rio Gran
GERMAN, ELWIN	164.00	250012381	370001537	300651463	Timeline	I-213	I-213	NGL6266613...	2021-06-07 03:51:47	USBP	Tucson S
WYNN, RIPKEN	164.00	250028365	389126678	300651854	Timeline	I-213	I-213	MCP3839043...	2021-06-23 03:51:47	OFO	Rio Gran
BRYAN BLAZE, CHAS-ROCHELLE	141.00	250010048	382989896	300651421	Timeline	I-213	I-213	CPC5889047...	2021-06-04 05:18:11	USBP	Rio Gran
HARROP, RANDI	141.00	250028842	389126571	300651747	Timeline	I-213	I-213	CPC5889047...	2021-06-23 03:51:47	OFO	Big Bend
JAMES, CLAIRE	141.00	250028246	389127007	300652183	Timeline	I-213	I-213	MCP3839043...	2021-06-23 03:51:47	USBP	LAREDO
SEGAL, JANE	141.00	250028730	389126961	300652137	Timeline	I-213	I-213	MCP3839043...	2021-06-23 03:51:47	USBP	LAREDO
YIELDS, JERRY	141.00	250128745	389126636	300651812	Timeline	I-213	I-213	MCP3839043...	2021-06-23 03:51:47	OFO	Rio Gran
BOY, MELIA ISABELLA-DANETTE	135.00	250034233	371950588	300651410	Timeline	I-213	I-213	CPC1940167...	2021-06-03 10:49:23	USBP	Rio Gran
DULING, OLIVER	135.00	252958745	389126625	300651801	Timeline	I-213	I-213	MCP3839043...	2021-06-23 03:51:47	OFO	Rio Gran
WENDELYN, SEYMOUR	135.00	236828745	389126811	300651987	Timeline	I-213	I-213	MCP3839043...	2021-06-23 03:51:47	OFO	LAREDO
ADDISON, KIMBERLY	119.00	250023965	389126721	300651897	Timeline	I-213	I-213	MCP3839043...	2021-06-23 03:51:47	OFO	LAREDO
GONZALEZ-RAMOS, TINA ROSA	102.00	219222930	219222001	2315874	Timeline	I-213	I-213	MCS0553913...	2021-06-01 06:44:35	USBP	McAllen
BEST, ADAM	93.00	250423456	389126775	300651951	Timeline	I-213	I-213	MCP3839043...	2021-06-23 03:51:47	OFO	LAREDO
MARGUERITE, ELIDA	93.00	250017430	362131576	300651560	Timeline	I-213	I-213	CPC3605740...	2021-06-13 22:49:23	USBP	Rio Gran
BRYAN BLAZE, CHAS-ROCHELLE	91.00	250010048	374120901	300651420	Timeline	I-213	I-213	CPC3675738	2021-06-04 03:37:23	USBP	Rio Gran

Figure Two: UIP Subject Pipeline Dashboard (mock data only)

As a visualization tool, UIP users may access and view an individual's general immigration encounter history, including interactions across multiple agencies, with icons that display changes in custody or status through the timeline view. The network view visualizes an individual's relationship to others in the immigration process (e.g., other individuals who are apprehended or in custody) and related events and connections throughout processing. Users are also able to drill down to a more detailed subject view to retrieve certain specific information about an individual (e.g., forms, medical logs, arrests). Users may also display information through map views, to visualize apprehension and custody locations, as well as identify patterns and activity trends in a certain geographic location.

The UIP replaces the need for agencies to initiate queries of numerous information technology systems when encountering an individual. Instead, encounters are now visually displayed in the portal in near real-time as an individual progresses through the immigration enforcement or benefits process (e.g., transfers from the custody of one agency to another).[3] Using the UIP also reduces the likelihood of human error by accessing and displaying data from multiple systems in near real-time. This enables users to conduct automated analysis of several databases simultaneously and reduces the need to manually compare data within separate locations. Data is pulled from various databases and displayed in a user-friendly manner (e.g., graphs, charts, tables) for users to easily comprehend the consolidated data. The UIP helps users perform searches of data (e.g., querying one or more databases simultaneously) or better understand the results of their searches (e.g., by using data visualization capabilities or performing quantitative or statistical analysis). Lastly, the UIP allows authorized users to structure the resulting information in a way that provides context and accurately interprets the data.

Data Sources

The UIP displays data using various tools to enable users to better access and visualize datasets already accessible by the respective agencies. The UIP accesses and displays certain information from DHS, DOJ, and HHS either through a direct system connection or through access to a data mart (e.g., Enterprise Management Information System-Enterprise Data Warehouse (EMIS-EDW)).[4] Appendix A of this Privacy Impact Assessment includes a list of the data sources in the UIP. CBP will routinely update this appendix as additional data sources are added to the UIP.

[3] As noted above, the Department of State (DOS) plays a key role in the immigration process. At the time of publication, UIP does not access DOS data. CBP will update this Privacy Impact Assessment, should UIP begin accessing and displaying DOS data.

[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE MANAGEMENT INFORMATION SYSTEM-ENTERPRISE DATA WAREHOUSE (EMIS-EDW), DHS/CBP/PIA-034, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

This Privacy Impact Assessment describes the approved services, dashboards, and use cases that encompass the UIP. All current use cases are consistent with immigration mission and authorities and conform to the purpose for which the data was originally collected. The UIP enables users to look at trends and patterns in data that are critical to immigration operations. At a high level, CBP and the other federal government stakeholder agencies anticipate using the UIP to assess existing data for the following use cases:

1. **Executive-Level Decision-Making:** U.S. government agencies are moving toward increasingly data-driven decision-making. The UIP provides agency leadership a platform to assess and visualize data about their specific areas of responsibility to make leadership and management decisions.
2. **Strategic Resource and Asset Allocation:** DHS, DOJ, and HHS are responsible for securing and safeguarding vast amounts of information, locations, personnel, and resources. The UIP will give agency field-level leadership a high-level view of the use of agency resources and assets, which will allow agencies to deploy resources more effectively.
3. **Custody and Apprehension Information Trends and Patterns:** DHS, which is responsible for immigration enforcement and for maintaining temporary custody of encountered noncitizens, requires better integration and faster, visual depictions of changes in patterns of encounters, increases or decreases in time in custody, and the volume and locations of individuals in custody.
4. **Immigration Process Flow Analysis:** DHS, DOJ, and HHS, who are each responsible for administering different aspects of the U.S. immigration system, require better integration to create a more complete picture or timeline of an individual's interactions with the U.S. immigration system.
5. **Law Enforcement Intelligence:** CBP and ICE's missions include identifying potential law enforcement and security risks and developing intelligence to counter those risks. The UIP allows these agency users to more easily identify individuals, associations, relationships, or patterns that may pose a potential law enforcement or security risk and assists users in the field in preventing violations of law or regulations at and/or between ports of entry.
6. **Contact Tracing:** Contact tracing allows agencies to proactively manage and respond to potential exposure to COVID-19 and other infectious diseases by rapidly producing a list of all individuals that a subject may have come into direct or indirect contact with during their time in custody. A contact tracing report can be exported from a subject's profile timeline, and this exposure network can be visualized on the Network View. In the UIP, contact tracing specifically relies on the booking/transfer data of individuals in CBP or ICE

custody and to identify individuals who are COVID-positive or COVID-risk via the United States Border Patrol (USBP) COVID-19 questionnaire.

7. **Data Services:** The UIP provides application programming interfaces (APIs) that allow system to system data exchanges. Relevant and timely data from a system of record can be shared to other systems to reduce manual data entry, expedite processing workflows, and provide visibility into prior or upcoming actions.
8. **Data Integration:** The UIP combines disparate data from across the immigration lifecycle into a central data store. Using the UIP as an immigration event log enables easier data integration and distribution of more complete data sets to agencies involved in the immigration process based on privacy agreements.

The above describes a high-level overview of the uses of the UIP. A more detailed description of the current use cases is included in Appendix B of this Privacy Impact Assessment. CBP requires the completion of a Privacy Threshold Analysis (PTA) for new use cases and will update Appendix B to this Privacy Impact Assessment if additional use cases are approved.

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 UIP is congressionally funded and mandated by the 2019 Emergency Supplemental Appropriations for Humanitarian Assistance and Security at the Southern Border Act (Pub. L. 116-26, 133 Stat. 1018). The UIP is used for purposes that support existing immigration, law enforcement, and border security authorities. Each agency that contributes data to the UIP collects and shares certain information pursuant to their own authorities. The information within the UIP that is originally covered by each individual contributing agency is covered under numerous authorities, including Title II of the Homeland Security Act of 2002 (Pub. L. 107-296, 116 Stat. 2135), as amended by the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108-458, 118 Stat. 3638); the Tariff Act of 1930 (Pub. L. 71-361, 46 Stat. 590), as amended; the Immigration and Nationality Act (“INA”) (Pub. L. 89-236, 79 Stat. 911), codified at 8 U.S.C. § 1101, et seq.; the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110-53, 121 Stat. 266); the Antiterrorism and Effective Death Penalty Act of 1996 (Pub. L. 104-132, 110 Stat. 1214); SAFE Port Act of 2006 (Pub. L. 109-347, 120 Stat. 1884); and the Aviation and Transportation Security Act of 2001 (Pub. L. 107-71, 115 Stat. 597)..

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

There are various System of Records Notices (SORN) that cover collection, use, maintenance, and dissemination of information within the UIP. These System of Records Notices are identified in Appendix A of this Privacy Impact Assessment.

The UIP itself does not generate or create any new records covered by the Privacy Act.

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

Yes. The UIP is a subsystem under the major application, Athena. Athena is accredited per the security authorization process (SAP) in accordance with the requirements defined under the Federal Information Security Management Act (FISMA). The most recent security authorization process for Athena was completed on May 2, 2019.

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

As a data visualization tool, the UIP retrieves and temporarily displays information from multiple source systems. The UIP deletes all information immediately at the end of a user's UIP session.

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.

The UIP is not subject to Paperwork Reduction Act requirements because it only uses information from other systems. However, information from source systems may be subject to the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

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

The UIP accesses and displays certain information from a variety of data sources to enable certain government agencies involved in the immigration process to receive and visualize the information for operational awareness. The UIP allows users to analyze and interpret existing data more effectively, without changing or impacting the integrity of the data in the original source system(s). The UIP adheres to approved datasets outlined in Appendix A of this Privacy Impact Assessment. Using this data, the UIP displays a visualization of data to show an individual's progress as they move through various stages of the immigration process, and improves access to information, as appropriate, for certain agencies involved in the immigration process. The data elements within the UIP include, but are not limited to the following information:

- Name;
- Address;
- Date of birth;
- Aliases;
- Age;
- Gender;
- A-Number;
- Fingerprint Identification Number (FIN);
- Subject ID;
- Event Number;
- Citizenship;
- Seizure information;
- Apprehension information;
- Detention information;
- Facility information;
- Criminality information (e.g., gang affiliation, prior convictions);
- Admissibility determination;
- Information regarding law enforcement actions, such as arrests (related to primary and secondary processing activities);
    - Date/Time of an action;
    - Action code; and
    - Location/facility code associated with an action.
- Medical Information, including indication of a medical screening;

- COVID-19 Screening-Related Information, including;
  - Symptoms (fever, cough, difficulty breathing, or other flu-like symptoms);
  - Subjects segregated and monitored as a precaution;
  - Subjects referred to a hospital for any flu-like symptoms;
  - CDC Consultations Conducted (Y/N);
  - Subjects traveled to/through/from an at-risk country within the last 14 days;
  - Subjects quarantined as per the CDC;
  - List the subject's travel details (e.g., dates, countries, method of travel);
  - COVID-19 Tests Conducted; and
  - COVID-19 Test Results.
- ICE arrest information;
- Transfer information;
- Bookout/Release information;
- Detention Care information, such as custodial actions;
- Family information (e.g., Separations, Family Relationships);
- Demographic (e.g., Unaccompanied Children (UC), Family Unit, Single Adults) and Classification information (e.g., Second or Third Apprehension, Persistent Subject);
- Program information (e.g., Migrant Protection Protocols (MPP), Operation Allies Welcome (OAW)); and
- Immigration Court information (e.g., Tentative Court Dates, Notice to Appear (NTA)).

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

The UIP replicates and displays information from CBP, USCIS, ICE, DOJ, and HHS source systems via a direct connection to those systems or through a connection to EMIS-EDW.[5] The information is originally collected by the respective agency in furtherance of their mission

[5] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE MANAGEMENT INFORMATION SYSTEM-ENTERPRISE DATA WAREHOUSE (EMIS-EDW), DHS/CBP/PIA-034, *available* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

and is shared amongst the agencies in furtherance of their respective immigration-related missions. UIP users use the tool to access information from partner agencies already accessible by their agency via data sharing agreement or policy. The UIP provides users with the ability to access and visualize existing data. The information within the UIP is generally a combination of information originally collected from the individual and information generated by the agency.

Appendix A to this Privacy Impact Assessment includes a list of data sources that the UIP accesses and displays. CBP will update this appendix as additional data sources are added.

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. The UIP does not collect, use, maintain, or disseminate information from commercial sources or publicly available information.

2.4 Discuss how accuracy of the data is ensured.

The information within the UIP is dependent on the accuracy and quality of data within the source systems and data mart. The UIP receives updates from the source systems on a near real-time basis to enable the display and visualization of data. The UIP also has an automated refresh function (e.g., every 30 minutes) to ensure the completeness of data within the portal. The refresh function identifies and captures any changes to data within a source system and updates the data in the UIP. The UIP does not alter or transform data in the source systems, and automated and manual quality checks are integrated into the tools to validate source data as it is ingested. The UIP does not retain any stale data; all previous data are overwritten during the refresh.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the UIP accesses and displays more information than necessary to accomplish the goal of the portal.

Mitigation: This risk is mitigated. Users are only able to access information that they are authorized to access. CBP employs tools and coordinates with partner agencies to manage the access controls for the data and define who within an organization has authority to access the data, and how the data may be used. These tools ensures that the UIP only displays certain information to users who are authorized to receive that information. With the implementation of the UIP, users can better visualize data they already have access to through other means. The UIP displays the information in a comprehensible way for better analysis and action.

Privacy Risk: There is a risk that the data in the UIP may be inaccurate, outdated, or be incorrectly associated with the wrong individual.

Mitigation: This risk is mitigated. The UIP receives and displays data directly from the source systems or through EMIS-EDW in near real-time. The UIP does not alter or transform the values of data in any way. Source systems routinely undergo rigorous automated and manual data quality checks. These data quality checks validate that the source system data is accurate, compete, and up to date as it is ingested and that it is properly associated with the correct individual based on unique identifiers. Further, when the UIP is refreshed old information that may no longer be accurate is overwritten with current data from the source systems.

Privacy Risk: There is a risk that information in previously generated reports may be outdated.

Mitigation: This risk is partially mitigated. Because the UIP accesses and receives information from the source system in near real-time, the reports UIP users create, save, or print only serve as a snapshot in time. However, because the UIP receives information in near real-time, users are encouraged to re-validate previously generated reports against UIP to confirm their accuracy.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The UIP, a visualization tool, provides a single interface for data sources from certain agencies involved in the immigration lifecycle to enable a more complete understanding of an individual's immigration journey. The UIP retrieves and temporarily displays certain information from multiple sources (e.g., CBP e3,[6] ICE Enforcement Integrated Database,[7] USCIS Global,[8] and HHS Unaccompanied Children PATH[9]) into dashboards. Dashboards provide users with the ability to see conditions at a high level (e.g., how many individuals are currently in custody). However, users can drill down further to retrieve details about a specific individual (e.g., name, A-Number, current location, reason in custody).

[6] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSEMENT FOR THE CBP PORTAL (e3) TO ENFORCE/IDENT, DHS/CBP/PIA-012, *available at* www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[7] *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/privacydocuments-ice.

[8] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE USCIS ASYLUM DIVISION, DHS/USCIS/PIA-027, *available at* https://www.dhs.gov/privacydocuments-uscis.

[9] *See* U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, PRIACY IMPACT ASSESSMENT FOR THE UNACCOMPANIED ALIEN CHILDREN PORTAL, P-9614390-049466, *available at* https://www.hhs.gov/sites/default/files/acf-uacp.pdf.

All use cases are consistent with the respective agencies' immigration-related mission and conform to the purpose for which the data was originally collected. The UIP enables users to look at trends and patterns in data that are critical to immigration operations. At a high level, CBP and the other agencies anticipate using the UIP to assess existing data in the following dashboards:

- **CBP Operational Dashboards:** This dashboard displays a bird's-eye view of the status of CBP migrant processing (e.g., whether a subject has been processed, if a placement request has been sent to HHS) and information related to CBP facilities (e.g., average/maximum processing time per facility, current number of individuals held by facility, sector, or state). The interactive nature of this dashboard enables users to drill down and display personally identifiable information (PII) such as name, address, date of birth, aliases, age, gender, A-File number, Fingerprint Identification Number, citizenship, visa number, and passport number.

- **CBP-ICE Subject Pipeline Dashboard:** This dashboard enhances current reporting methods that rely on disparate CBP and ICE data sources. While existing tools fulfill the requirements to track individual migrants in custody, the tools lack the ability to quickly create a snapshot of CBP operations. This dashboard provides a rapid assessment and operational view of the number of individuals in CBP custody. This information allows ICE to gain awareness of current CBP operational conditions and prepare for individuals who may be transferred into ICE custody. This is currently a limited scope use-case for a comprehensive dashboard for CBP and ICE senior leadership.

- **Migrant Protection Protocol (MPP) Dashboard:** This dashboard provides data on noncitizens who are processed under the Migrant Protection Protocol Program.[10] The dashboard combines CBP processing data with USCIS Migrant Protection Protocol non-refoulement interview case outcomes, thereby giving the users a complete picture of Migrant Protection Protocol cases.[11] ICE also accesses this dashboard.

[10] The Migrant Protection Protocols are a U.S. Government action whereby certain foreign individuals who sought to enter or seek admission to the U.S. from Mexico—illegally or without proper documentation—are returned to Mexico for the duration of the immigration proceedings. For more information about CBP's efforts with the Migrant Protection Protocol Program, *see* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSEMENT FOR THE PROCESSING INDIVIDUALS SUBJECT TO MIGRANT PROTECTION PROTOCOLS, DHS/CBP/PIA-070, *available at* www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[11] Section 235 of Immigration and Nationality Act (INA), as amended, and its implementing regulations provide that certain categories of individuals are subject to expedited removal without a hearing before an immigration judge. Individuals subject to expedited removal who indicate an intention to apply for asylum, express a fear of persecution or torture, or a fear of return to their home country are referred to USCIS asylum officers to determine whether the individual has a credible fear of persecution or torture. Individuals determined to have a positive credible fear of persecution or torture are placed into removal proceedings under INA § 240 by the issuance of a Notice to Appear and may apply for asylum as a defense to removal before an immigration judge.

- **<u>Unaccompanied Children (UC) Dashboard</u>:** This dashboard enables HHS to better prepare for the transfer of Unaccompanied Children and enables improved resource allocation across all government stakeholders. The dashboard allows HHS users to rapidly assess the demographic information of Unaccompanied Children who are in CBP custody awaiting placement, so that HHS may improve coordination with CBP and quickly determine appropriate placement for each Unaccompanied Child. The dashboard also provides awareness to authorized personnel at DHS Headquarters (HQ), the Federal Emergency Management Agency (FEMA), ICE, and USCIS.

CBP will add an appendix to this Privacy Impact Assessment if additional use cases are approved.

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. However, the UIP enables users to better visualize immigration trends and patterns that are critical to the federal agencies that support the U.S. immigration system.

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

Yes. DHS HQ, FEMA, ICE, and USCIS have access to the UIP. ICE and USCIS are contributors to and users of the portal. Authorized users at DHS HQ and FEMA have access to the portal for situational awareness.

3.4 <u>Privacy Impact Analysis</u>: Related to the Uses of Information

<u>Privacy Risk</u>: There is a risk that a user will use the information visualized in the UIP for unapproved uses.

<u>Mitigation</u>: This risk is mitigated. CBP, ICE, USCIS, DOJ, and HHS users (as well as other approved DHS and non-DHS agency partners) use the UIP for a variety of approved uses, including to make data-driven decisions about resource or asset allocation. All current use cases are consistent with each user agency's immigration-related mission and authorities and conform to the purpose for which the data was originally collected. The UIP enables users to look at trends and patterns in data that are critical to immigration operations. Sharing immigration-related information amongst other agencies with an immigration responsibility is crucial to making impactful and mission-critical decisions. Furthermore, the UIP's access and use of source data does not change the circumstances of, or purpose for, the collection of the original information. The UIP provides new technical capabilities which support each user agency's existing use and understanding of its information, but it does not change the purpose for which each agency collects and uses the information. The use cases included in this Privacy Impact Assessment have been reviewed and approved by CBP's Privacy and Diversity Office and CBP's Office of Chief Counsel. CBP will continue to review new uses through the PTA process. Should additional uses beyond what is included in this Privacy Impact Assessment be approved, CBP will add an appendix to this Privacy Impact Assessment.

Section 4.0 Notice

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 are provided general notice of the UIP through this Privacy Impact Assessment, source system Privacy Impact Assessments, and other component/agency Privacy Impact Assessments. The System of Records Notices applicable to the data visualized in the UIP also provide additional transparency. Moreover, when CBP collects information from persons entering the United States, CBP provides a form of notice by using multiple signs in the publicly accessible areas at ports of entry. Individuals encountered between ports of entry may not be provided advance notice but will be provided general notice at the time the information is collected (e.g., during an inspection, apprehension). In addition, many of the forms DHS and other federal agencies use to collect information include a Privacy Act Statement or Privacy Notice.

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

Individuals do not have the opportunity to consent to the uses of their information in the UIP because the UIP is not a source system. Furthermore, CBP does not offer individuals an opportunity to decline to provide or use their information, due to the circumstances of encounters and purpose for collecting the information—immigration and law enforcement.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not be aware that CBP is using their data within the UIP.

Mitigation: This risk is partially mitigated. CBP is providing notice of the use of the UIP through the publication of this Privacy Impact Assessment. In addition to this Privacy Impact Assessment, CBP, ICE, and USCIS have issued several system and programmatic Privacy Impact Assessments that discuss the datasets included in UIP. All DHS compliance documents are available at www.dhs.gov/privacy. In addition to these DHS compliance documents, HHS and

DOJ have also issued Privacy Impact Assessments related to their datasets.[12] However, as described above, while the UIP provides new technical capabilities which support each user agency's existing use and understanding of its information, it does not change the purpose for which each agency uses the information.

Section 5.0 Data Retention by the Project

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

The UIP retrieves and displays information from other source systems. The UIP then deletes all information immediately at the end of a user's UIP session.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the UIP will retain data for longer than is necessary.

Mitigation: This risk is mitigated. The UIP does not retain data once the user logs off the UIP. In cases in which a user chooses to retain the results of any data analysis in reports or in some other format, the retention must be consistent with the applicable System of Records Notices for the work product. Typically, users maintain UIP outputs (such as electronic results or written analysis) in a shared space (e.g., access-controlled SharePoint sites) in which users may collaborate with each other. This storage of results must also be consistent with the System of Records Notices that cover the user's analytical results. UIP users are required to acknowledge the Terms of Use each time they log onto UIP. The Terms of Use outlines the user's responsibilities and provides the user notice that unauthorized or improper use or access may result in disciplinary action, as well as civil and criminal penalties.

[12] HHS Privacy Impact Assessments are available at: https://www.hhs.gov/pia/index.html. At the publication of this Privacy Impact Assessment, no EOIR data is within UIP. However, CBP eventually plans to ingest EOIR data into UIP. DOJ Privacy Impact Assessments are available at: https://www.justice.gov/opcl/doj-privacy-impact-assessments.

Section 6.0 Information Sharing

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, ICE, USCIS, HHS, and DOJ routinely share and receive information with one another throughout the immigration lifecycle. The UIP enables these agencies to publish data from their respective agency's immigration IT systems to the UIP. The UIP then consolidates and displays the combined multiagency data in several user-friendly formats to enable users to combine and connect the data and display it using visualization tools. The UIP allows partner agencies to see records they already have access to through a single streamlined window. The UIP does not share or provide access to any new data.

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

As noted above, the UIP displays information that external agency users can already access. There are various DHS System of Records Notices and Routine Uses within those System of Records Notices that cover the collection and sharing of information with DOJ and HHS. The sharing of information is compatible with the purpose for which the information is collected because like CBP, both DOJ and HHS have a role in the U.S. immigration system. For instance, HHS-ORR is responsible for the care and custody of Unaccompanied Children transferred from CBP custody to its custody. DOJ EOIR is charged with administering immigration court proceedings.

6.3 Does the project place limitations on re-dissemination?

Yes. A Memorandum of Understanding/Agreement (MOU/A) exists between DHS and DOJ and HHS, respectively, that places limitations on re-dissemination of information. DOJ and HHS may only share information under the MOU/A when the recipient has an official need—in accordance with the terms of the MOU/A—is allowed by applicable privacy and confidentiality statutes and is permitted by CBP.

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

The UIP provides agencies involved in the immigration process a means to view and access each of the respective agencies' information from a single view. The UIP maintains audit logs to capture what data was accessed by each individual user.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the UIP will display more information through the UIP than DOJ and HHS previously had access to.

Mitigation: This risk is mitigated. CBP carefully evaluated the existing HHS and DOJ information sharing agreements to ensure the information HHS and DOJ accesses aligns with the prior arrangements. The agreements between DHS and DOJ and HHS, respectively, fully outline responsibilities of the parties, security standards, and limits of use of the information, including re-dissemination, prior to information sharing. Records are kept as system audit trail logs, which are maintained to identify transactions performed by users. Furthermore, CBP ensures through the MOU/A process that the external agencies have policies, procedures, and training in place to provide safeguards that information is not inappropriately disseminated. In addition to the information sharing agreements, CBP reviews the routine uses in the applicable System of Records Notices to verify the compatibility of an information exchange prior to disclosing data. Finally, UIP users are required to acknowledge the Terms of Use each time they log onto UIP. The Terms of Use outlines the user's responsibilities, including that unauthorized or improper use or access may result in disciplinary action, as well as civil and criminal penalties.

Section 7.0 Redress

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

Individuals seeking notification of and access to information contained in CBP records may gain access to certain information by filing a Freedom of Information Act (FOIA) request with CBP at https://foia.cbp.gov/, 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, D.C. 20229
Fax Number: (202) 325-1476

U.S. citizens, lawful permanent residents, and individuals who have records covered under the Judicial Redress Act (JRA) may file a Privacy Act request to access their information. CBP will refer requests for information contained in immigration systems maintained by other DHS components or by HHS or DOJ to those agencies for additional processing.

All Privacy Act and Freedom of Information Act requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. Requests for information are evaluated by CBP to ensure that the release of information is lawful; will not impede an investigation of an actual or potential criminal, civil, or regulatory violation; and will not reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

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

Individuals can correct their inaccurate or erroneous information in CBP records. During interactions with CBP, individuals can inform CBP officers and agents of inaccurate information if they are asked a question that contains inaccurate information. In addition, individuals can review and sign some of the forms CBP creates during processing and they can inform CBP officers and agents of any inaccurate information in the forms.

A person who believes that CBP's actions are the result of incorrect or inaccurate information may request information about his or her records pursuant to procedures provided by the Freedom of Information Act. U.S. citizens, lawful permanent residents, and individuals who have records covered under the Judicial Redress Act who believe that CBP's actions are the result of incorrect or inaccurate information may request correction of that data under the amendment provisions of the Privacy Act of 1974 by writing to the above address. The CBP Privacy Division reviews all requests for correction and amendment regardless of status. CBP will refer requests for information contained in immigration systems maintained by other DHS components or by HHS or DOJ to those agencies for additional processing.

Travelers may also contact the DHS Traveler Redress Inquiry Program (TRIP) at 601 South 12th Street, TSA-901, Arlington, VA, 22202-4220 or online at www.dhs.gov/trip. Individuals making inquiries should provide as much identifying information as possible to identify the record(s) at issue.

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

Individuals are notified of the procedures for correcting their information through the System of Records Notices describing each of the underlying systems from which the UIP accesses information. This Privacy Impact Assessment also serves as notification. Additionally, signage and tear sheets at ports of entry provide information on how to contact the DHS Traveler Redress Inquiry Program. In addition, travelers may request information from the on-site CBP officer.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals whose information is within the UIP will not know how to submit redress requests.

Mitigation: This risk is partially mitigated. This Privacy Impact Assessment provides information on how to request access and amendments to CBP information. Additionally, CBP officers inform travelers verbally and through tear sheets on how they can challenge a determination and request information CBP used to make a determination. Travelers who wish to access information about themselves or challenge a determination can submit a Freedom of Information Act request to CBP or a Traveler Redress Inquiry Program request to the Transportation Security Administration (TSA) via the addresses above. Additionally, U.S. citizens, lawful permanent residents, and individuals covered by the Judicial Redress Act, may submit a Privacy Act Amendment request to CBP.

Section 8.0 Auditing and Accountability

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

CBP is following DHS requirements for information assurance and security for the UIP dashboards. The dashboards either have undergone a DHS security review to ensure DHS standards for security policy, guidance, and architecture requirements have been or will be met before use cases, data from source systems, or new tools are approved. All tools, data, and uses were included in the security Authority to Operate (ATO) package and approved by the DHS Chief Information Security Officer (CISO).

The UIP uses audit logging so that user requests and the results returned in response to those requests will be logged and include date and timestamps of these transactions. Each underlying source system maintains a list of users; each list is reviewed annually with system access rights removed for those users no longer needing access.

All users of the system must have access approved by their supervisor and the system access supervisor (both of which are government positions). These supervisor and system access approvers have a responsibility to validate whether the individual requesting access is authorized to access the system.

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

The UIP connects to underlying source systems, each of which has its own approved privacy documentation that outlines specific training and auditing requirements for that individual system. CBP provides mandatory privacy training to all employees and contractors who have access to or use PII, and all users are required to complete information security training that addresses privacy as well as the proper and secure use of DHS applications. In addition, the CBP Privacy and Diversity Office offers role-based training for agency employees involved with information sharing.

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

UIP users will only be able to access data for which they have received authorization. In other words, UIP users must be separately authorized to access the underlying source system data to access data within a particular dashboard. UIP employs tools to enforce access control policies outlined by the respective agency, system owner, mission-area, policy, and/or information sharing agreements. Each agency’s data owners are responsible for defining access controls in accordance with policies and information sharing agreements. With these access controls in place, the UIP will only display information and data elements that are authorized to be accessed by that particular user. The UIP will not be able to display information beyond what the individual user is authorized to access. Should additional access be required by an existing category of users or a new type of user, the request will be processed in accordance with established access control policies and procedures at the source system or database and will be documented in an approved mission use case. All users of the UIP have read-only access to the source data and cannot change the underlying data.

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 information sharing agreements for this data defines the nature of access, the scope of information subject to the sharing agreement, and the privacy, security, safeguarding, and other requirements. All information sharing arrangements are reviewed by the CBP Privacy Officer and the CBP Office of Chief Counsel in accordance with existing CBP and DHS policy.

Privacy Risk: There is a risk that individuals who are not normally authorized to access external data sets will be able to gain access to data through the UIP.

Mitigation: This risk is mitigated. CBP, in coordination with the partner agencies, controls access to the datasets and dashboards within UIP. CBP works with the partner agencies to determine what UIP user agencies should have access to their data. For example, CBP works with HHS to determine whether USCIS should have access to HHS data and what datasets they should or should not access in accordance with the respective information sharing agreements. Furthermore, users can only access UIP using validated, logged, and Identity, Credential, and Access Management (ICAM) controlled credentials. This ensures that only authorized U.S. government personnel may access the system.

Responsible Official

David K. Hansen
Acting Executive Director
Border Enforcement Management Systems
Office of Information Technology
U.S. Customs and Border Protection

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

Approval Signature

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

____

Lynn Dupree
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Appendix A: UIP Datasets

Last Updated: October 24, 2023

The UIP accesses and displays most source information via the Enterprise Management Information System-Enterprise Data Warehouse (EMIS-EDW).[13] EMIS-EDW extracts and consolidates current and historical data from various DHS source systems to present timely statistics, trend analysis for situational awareness, and the making of critical organizational decisions. In addition to accessing and receiving information via EMIS-EDW, the UIP directly connects to systems.

UIP accesses and displays information from the following systems:

A. DHS Systems

1. CBP Seized Assets and Case Tracking System (SEACATS)

SEACATS is the information system of record for the full lifecycle of all enforcement incidents related to CBP and U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) operations. The system tracks the physical inventory and records disposition of all seized assets, as well as the administrative and criminal cases associated with those seizures, and functions as the case management system capturing the relevant information and adjudication of the legal outcomes of all fines, penalties, and liquidated damages. The system also serves as the financial system of record for all collections related to these enforcement actions. In general, individuals whose information is included in this system include current, former, alleged, or suspected violators of customs, immigration, agriculture, or other laws and regulations administered or enforced by CBP. In addition, this system maintains information related to parties involved in, affected by, or queried concerning the violation of customs, immigration, agriculture, or other laws enforced or administered by CBP.

- PIA: DHS/CBP/PIA-040 Seized Assets and Case Tracking System[14]
- Associated SORN(s): DHS/CBP-013 Seized Assets and Case Tracking System[15]

[13] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE MANAGEMENT INFORMATION SYSTEM-ENTERPRISE DATA WAREHOUSE (EMIS-EDW), DHS/CBP/PIA-034, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[14] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE SEIZED ASSETS AND CASE TRACKING, DHS/CBP/PIA-040, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[15] *See* DHS/CBP-013 Seized Assets and Case Tracking System, 73 FR 77764 (December 19, 2008).

2. CBP Portal (E3) to ENFORCE/IDENT

CBP uses the e3 portal (e3) to collect and transmit data to ICE's Enforcement Integrated Database (EID)**[16]** and DHS's Automated Biometric Identification System (IDENT)**[17]** 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 suite of applications, which communicate with each other over the CBP network and through EID, enables CBP Border Patrol Agents to record an apprehended individual's biographic information and seized property; uniquely identify or verify the identity of encountered individuals by capturing photographs 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.

- PIAs:
  - DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT[18]
  - DHS/ICE/PIA-015 Enforcement Integrated Database (EID)[19]
  - DHS/OBIM/PIA-002 IDENT[20]
- Associated SORN(s):

[16] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSEMENT FOR THE ENFORCEMENT INTEGRATED DATABASE, DHS/ICE/PIA-015, *available at* www.dhs.gov/privacy-documents-us-immigrations-customs-enforcement. *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 FR 72080 (October 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.
[17] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM, DHS/OBIM/PIA-002, *available at* www.dhs.gov/privacy-documents-office-biometric-identity-management. DHS is retiring IDENT and replacing it with the Homeland Advanced Recognition Technology System (HART).
[18] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE CBP PORTAL (E3) TO ENFORCE, DHS/CBP/PIA-012 (2017 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[19] *See* supra note 11.
[20] *See* supra note 12.

  - DHS/CBP-023 Border Patrol Enforcement Records System of Records (BPER)[21]
  - DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records October[22]

3. eGIS

eGIS facilitates the integration of multiple CBP enforcement systems to expose spatial patterns and trends and provides CBP with mission critical features, including real-time intrusion sensor alerts; arrest and interdiction locations; assault and significant incident tracking; facility and infrastructure data; field information reports; and recidivist arrest analysis. eGIS helps CBP in identifying trends in border incidents to better inform staffing and event responses. eGIS uses data to create maps from multiple data sources, identify patterns and trends, and enhance traditional tabular reporting capabilities. eGIS depicts border resources and activities to facilitate situational awareness. eGIS provides authorized users with the ability to view the geographic location of data from various source systems as features on a map. eGIS is used to display information already available to law enforcement users through their access to various enforcement systems on a map for ease of use and to identity patterns and trends of illicit activity. Users can click on the features to view attribute information of the event, which may include PII. Generally, the types of attribute information within eGIS include historic enforcement, surveillance, intelligence, officer safety, and human resources data, as well as publicly available geospatial and landowner parcel contact information.

- PIAs:
  - DHS/CBP/PIA-041 Enterprise Geospatial Information Services (eGIS)[23]
- Associated SORN:
  - DHS/CBP-024 Intelligence Records System (CIRS) System of Records[24]

4. Intelligent Computer Assisted Detection (ICAD)

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

[22] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 FR 72080 (October 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

[23] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE GEOSPAITAL INFORMATION SERVICES (eGIS), DHS/CBP/PIA-041, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[24] *See* DHS/CBP-024 Intelligence Records Systems (CIRS) System of Records, 85 FR 80806 (December 14, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.

ICAD is a suite of software applications that assist the USBP in managing officer safety, detection device inventory, and real-time situational awareness and analysis along the borders. ICAD utilizes a myriad of sensor devices, cameras, and technologies that converge into a single stream of detection events in ICAD applications. ICAD utilizes technology to detect the presence or movement of individuals and relays that information to U.S Border Patrol Sector Headquarters. ICAD records the date, time, and location of the activity, as well as details input by the Border Patrol Agent investigating the incident. Border Patrol Agents input details including name, date of birth, document number, license plate number, and other biographic data about individuals encountered through ICAD detections. The sensor data is stored and can be retrieved by date, time, or the PII that is included in the incident details. Tracking Sign-cutting & Modeling (TSM), which is part of the ICAD suite, which provides a real-time record of sign-cutting,[25] spatial representation, and tracking operations. ICAD integrates with e3, eGIS, and BPETS to facilitate consistent and comprehensive monitoring of ground detection and geospatial tracking operations.

- PIAs:
    - DHS/CBP/PIA-022 Border Surveillance Systems (BSS)[26]
- Associated SORNs:
    - DHS/CBP-023 Border Patrol Enforcement Records (BPER)[27]
    - DHS/CBP-011 TECS[28]

5. Bond Management Information System (BMIS)

The Bond Management Information System (BMIS) is an immigration bond management database used primarily by the Office of Financial Management (OFM) at ICE. The basic function of BMIS is to support the financial management of immigration bonds posted for the release of noncitizens in ICE custody. Among other things, ICE uses BMIS to calculate and pay interest to obligors who post cash immigration bonds. Under Internal Revenue Service (IRS) rules, interest payments to certain obligors are subject to backup withholdings where a percentage of the payment is withheld as tax and sent to the IRS.

- PIAs:

[25] A sign is a type of foot-print or other descriptive attribute used to track a subject.
[26] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE BORDER SURVEILLANCE SYSTEMS, DHS/CBP/PIA-022, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[27] *See supra* note 16.
[28] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008), *available at* https://www.dhs.gov/system-records-notices-sorns.

    - DHS/ICE/PIA-005 Bond Management Information System Web Version (BMIS Web) 2.2[29]
- Associated SORNs:
    - DHS/ICE-004 - Bond Management Information System (BMIS)[30]

6. Information Technology Service Management (ITSM) – ServiceNow

The ICE Office of the Chief Information Officer (OCIO) operates the Information Technology Service Management (ITSM) - ServiceNow enterprise solution (ServiceNow). To better support its mission of streamlining the management of time-sensitive service requests, OCIO implemented a software as a service (SaaS) cloud-based tool that can be customized based on the needs of ICE program offices to provide support to ICE personnel (i.e., employees, contractors) and non-ICE personnel who have access to ICE systems for official business. ICE is publishing this Privacy Impact Assessment (PIA) to provide a thorough analysis of the privacy risks associated with ServiceNow's collection, use, and maintenance of personally identifiable information (PII).

- PIAs:
    - DHS/ICE/PIA-059 Information Technology Service Management - ServiceNow[31]

- Associated SORNs:
    - DHS/ALL-004 General Information Technology Access Account Records System (GITAARS)[32]
    - DHS/ALL-026 Department of Homeland Security Personnel Identity Verification Management System[33]

[29] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE BOND MANAGEMENT INFORMATION SYSTEM, DHS/ICE/PIA-005, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[30] *See* DHS/ICE-004 Bond Management Information System, 85 FR 64515 (October 13, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.

[31] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE INFORMATION TECHNOLOGY SERVICE MANAGEMENT – SERVICENOW, DHS/ICE/PIA-059, *available at* https://www.dhs.gov/privacy-documents-ice.

[32] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.

[33] *See* DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System, 74 FR 30301 (June 25, 2009), *available at* https://www.dhs.gov/system-records-notices-sorns.

- DHS/ALL-033 Reasonable Accommodations Records System[34]
- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER)[35]
- DHS/ICE-013 Alien Health Records System[36]
- OPM/GOVT-1 General Personnel Records[37]

7. USCIS Person Centric Query Service (PCQS)

The Person Centric Query Service (PCQS) allows DHS employees and certain external Federal agency employees, such as Department of State (DOS) Consular Officers, to obtain a consolidated read-only view of an immigrant or nonimmigrant's past interactions with the U.S. Government as he or she passed through the U.S. immigration system. PCQS retrieves and temporarily displays information from connected systems, which include USCIS systems, DHS systems, external agency systems, and private sector systems. PCQS presents a single access point and eliminates the need to access these individual systems separately.

PCQS does not store data. PCQS retrieves and temporarily displays information related to immigrants and relevant information for the immigration process, such as but not limited to enforcement incidents; travel history; family and beneficiary information. The information is retrieved from connected systems and displayed in a consolidated, read-only format for the user. Users initiate a PCQS search by entering a data element or a combination of data elements to uniquely identify a record in the connected IT system. Connected USCIS Systems include: Alien Change of Address Card (AR-11) System; Benefits Biometrics Support System (BBSS); Central Index System (CIS); Computer Linked Application Information Management System 3 (CLAIMS 3); Computer Linked Application Information Management System 4 (CLAIMS 4); Customer Profile Management System (CPMS); Enterprise Citizenship and Information Services Centralized Operational Repository – Central Index System (eCISCOR-CIS); Enterprise Citizenship and Information Services Centralized Operational Repository – Computer-Linked Application Management Information System CLAIMS 3 Local Area Network (eCISCOR–C3 LAN); Enterprise Citizenship and Information Services Centralized Operational Repository-Reengineered Naturalization Applications Casework Systems (eCISCOR-RNACS); Enterprise Citizenship and Information Services Centralized Operational Repository – Refugees, Asylum, and Parole System (eCISCOR-RAPS); FD 258 Fingerprint Tracking System; Marriage Fraud

[34] *See* DHS/ALL-033 Reasonable Accommodations Records System of Records, 76 FR 41274 (July 13, 2011), *available at* https://www.dhs.gov/system-records-notices-sorns.
[35] *See supra* note 17.
[36] *See* DHS/ICE-013 Alien Health Records System, 83 FR 12015 (March 19, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.
[37] *See* OPM/GOVT-1 General Personnel Records, 77 FR 73694 (December 11, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.

Amendment System (MFAS); National File Tracking System (NFTS); Refugees, Asylum, and Parole System (USCIS ELIS). Connected DHS Systems include: Arrival and Departure Information System (ADIS); Automated Biometric Identification System (IDENT); Automated Targeting System – Passenger (ATS-P); Enforcement Integrated Database (EID); Student and Exchange Visitor Information System (SEVIS); TECS (not an acronym). External systems include the American Association of Motor Vehicle Administrators (AAMVA) Network Service (AAMV Anet); Consular Consolidated Database (CCD); and Executive Office for Immigration Review (EOIR).

- PIA:
  - DHS/USCIS/PIA-010 Person Centric Query Service[38]
- Associated SORN(s):
  - SORN dependent on source system, however, DHS/USCIS-007 Benefits Information System[39] covers most of the information within PCQS.

8. USCIS Global

As the primary case management system for the USCIS Asylum Division, Global contains information pertinent to subjects seeking protection in the United States who have suffered past persecution or have a well-founded fear of future persecution in their country of origin, as outlined under Section 208 of the Immigration and Nationality Act (INA) (8 U.S.C. § 1158) and 8 CFR Part 208. The system also contains information pertinent to claims of protection from Mexico from certain individuals who were amenable to the Migrant Protection Protocols (MPP) and for whom USCIS conducted non-refoulement interviews. The USCIS Asylum Division also adjudicates the benefit program established by the Nicaraguan Adjustment and Central American Relief Act (NACARA) § 203 and administers safe third country, credible fear, and reasonable fear screening processes.

- PIA:
- DHS/USCIS/PIA-027(d) USCIS Asylum Division - September 2018[40]Associated SORN(s):

[38] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE PERSON CENTRIC QUERY SERVICE, DHS/USCIS/PIA-010, *available at* https://www.dhs.gov/privacy-documents-us-citizenship-immigration-services

[39] *See* DHS/USCIS-007 Benefits Information System, 84 FR 54622, (October 10, 2019), *available at* https://www.dhs.gov/system-records-notices-sorns.

[40] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE USCIS ASYLUM DIVISION, DHS/USCIS/PIA-027, *available at* https://www.dhs.gov/privacy-documents-us-citizenship-immigration-services.

- DHS/USCIS-001 Alien File, Index, and National File Tracking System of Records[41]
- DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records[42]
- DHS/USCIS-010 Asylum Information and Pre-Screening System of Records[43]

B. Non-DHS System/Sources

1. Department of Health and Human Services (HHS) Unaccompanied Children (UC) PATH Portal

The HHS UC PATH Portal was developed by HHS to manage information regarding the placement and care of UC's apprehended by CBP. The UC Portal enables HHS to track the statuses of both facilities and subjects, assisting the process of finding appropriate and available Office of Refugee Resettlement (ORR) facilities as well as local U.S. sponsors for every UC. The UC portal collects and stores information related to UC and their sponsors in the United States, some of whom may be U.S. citizens. Historically, HHS has provided CBP with a daily spreadsheet with information extracted from the UC portal. In addition to biographical data and contact information for UC and their sponsors, the UC Portal contains data related to the enforcement incident as well as placement process and requirements.

- PIA: HHS PIA for the Unaccompanied Children PATH Portal[44]
- Applicable SORN: 09-80-0321 ORR Division of Children's Services Records[45]

2. Department of Justice (DOJ) EOIR Courts and Appeals System (ECAS)

DOJ ECAS is a case management system with document management and research functionality that supports immigration judges and Board of Immigration (BIA) Board members

[41] *See* DHS/USCIS-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (November 22, 2013), *available at* https://www.dhs.gov/system-records-notices-sorns.

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

[43] *See* DHS/USCIS-0010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (November 30, 2015), *available at* https://www.dhs.gov/system-records-notices-sorns.

[44] *See* U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES PRIVACY IMPACT ASSESSMENT FOR THE UNACCOMPANIED ALIEN CHILDREN PORTAL, PIA Unique Identifier: P-9614390-049466, *available at* https://www.hhs.gov/sites/default/files/acf-uacp.pdf.

[45] 09-80-0321 ORR Division of Children's Services Records, 81 FR 46683 (November 18, 2016), 83 FR 6591 (February 14, 2018), *available at* https://www.hhs.gov/foia/privacy/sorns/acf-sorns.html.

and their personnel in hearing cases, researching matters, and drafting and finalizing decisions. ECAS is available at all immigration courts and the Board of Immigration Appeals. ECAS enables DHS to file court and appear documents, including Notices to Appear (NTAs). UIP interacts with ECAS by automating the scheduling of court dates and filing of court documents.

- PIA: EOIR eWorld Adjudication System[46]
- Associated SORN(s):
    - JUSTICE/EOIR-001 Records and Management Information System[47]
    - JUSTICE/EOIR-003 Practitioner Complaint-Disciplinary Files[48]
    - JUSTICE/BIA-001 Decisions of the Board of Immigration Appeals[49]
    - JUSTICE/BIA-002 Roster of Organizations and their Accredited Representatives Recognized by the Board of Immigration Appeals[50]
    - JUSTICE/DOJ-002 DOJ Computer Systems Activity & Access Records[51]
    - JUSTICE/DOJ-003 Correspondence Management Systems (CMS) for the Department of Justice[52]
    - JUSTICE/DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records[53]
    - DOJ-011Access Control System (ACS)[54]

[46] *See* DEPARTMENT OF JUSTICE, EXECUTIVE OFFICE FOR IMMIGRATION REVIEW, PRIVACY IMPACT ASSESSMENT FOR THE EWORLD ADJUDICATION SYSTEM, *available at* https://www.justice.gov/opcl/doj-privacy-impact-assessments.

[47] *See* JUSTICE/EOIR-001, Records and Management Information System, 81 Fed. Reg. 24147 (May 25, 2017), *available at* https://www.justice.gov/opcl/doj-systems-records.

[48] *See* JUSTICE/EOIR-003, Practitioner Complaint-Disciplinary Files, 82 Fed. Reg. 24147 (May 25, 2017), *available at* https://www.justice.gov/opcl/doj-systems-records.

[49] *See* JUSTICE/BIA-001, Decisions of the Board of Immigration Appeals, 82 Fed. Reg. 24147 (May 25, 2017), *available at* https://www.justice.gov/opcl/doj-systems-records.

[50] See JUSTICE/BIA-002, Roster of Organizations and their Accredited Representatives Recognized by the Board of Immigration Appeals, 82 Fed. Reg. 24147 (May 25, 2017), available at https://www.justice.gov/opcl/doj-systems-records.

[51] *See* JUSTICE/DOJ-002, DOJ Computer Systems Activity and Access Records, 82 Fed. Reg. 24147 (May 25, 2017), *available at* https://www.justice.gov/opcl/doj-systems-records.

[52] *See* JUSTICE/DOJ-003, Correspondence Management Systems (CMS) for the Department of Justice, 82 Fed. Reg. 24147 (May 25, 2017), *available at* https://www.justice.gov/opcl/doj-systems-records.

[53] *See* JUSTICE/DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records, 82 Fed. Reg. 24151 (May 25, 2017), *available at* https://www.justice.gov/opcl/doj-systems-records.

[54] *See* JUSTICE/DOJ-011, Access Control System (ACS), 82 Fed. Reg. 24147 (May 25, 2017), *available at* https://www.justice.gov/opcl/doj-systems-records.

Appendix B: UIP Services and Data Integration

1. ID Exchange

    - **Overview:** The ID Exchange (IDX) facilitates records matching across the immigration lifecycle by providing identifiers for a subject. The user provides an input identifier (e.g., an A-Number) and receives matching identifiers for that subject in return (e.g., a subject ID). This service expedites processing by removing the need for manual look-ups and identity resolution across immigration records, court orders, or narratives. This reduces the possibility of data entry error and provides traceability of record matching.
    - **Users:** CBP, DHS, DOJ, HHS, ICE, USCIS

2. UC Referral Service

    - **Overview:** When an Unaccompanied Child (UC) enters the immigration system, several agencies work together to move the UC quickly and safely to an HHS facility that can provide appropriate care and custody for the child pending release to a sponsor. Timely and accurate information is critical. The UC referral service enables CBP and ICE to request a facility placement from HHS, and for HHS to provide placement confirmation and share placement details. This automates and unifies currently disparate workflows into a single data exchange to improve transparency on UC status and expedite communication across agencies, which is required to align resources for UC care. It reduces the need for e-mail back and forth and for manual data entry.
    - **Users:** CBP, DOJ, HHS, ICE, USCIS

3. UIP Biographic Service

    - **Overview:** The UIP Biographic Service provides biographical details about a person in the immigration lifecycle. The service enables timely and secure system-to-system data sharing to reduce the manual effort required to respond to inquiries or requests for information (RFIs). The consumer provides an input identifier (e.g., subject ID) and receives information such as name, A-Number, country of citizenship, date of birth, gender, location, and age.
    - **Users:** CBP, DOJ, HHS, ICE, USCIS

4. Web Emergency Operations Center (WebEOC) Electronic Medical Records (EMR)

    - **Overview:** CBP has a time critical need across the Southwest Border of the U.S. to capture medical health information for individuals in CBP custody. The WebEOC supports emergency management processes and functions by providing a real-time common operating picture to perform incident management, coordination, and situation awareness functions, including the collection, maintenance, and generation of records of medical screening and treatment provided to individuals while they are in short-term CBP custody. CBP will leverage the WebEOC EMR board to track medical health information. This medical health information includes medical intake, medical assessments, and record follow-up and monitoring actions for individuals in CBP custody. To streamline this process and reduce the risk of data errors and redundancy, CBP will use the UIP to share limited biographic data with the WebEOC EMR board.

- **Users:** CBP

5. <u>Electronic Notice to Appear (eNTA) Service</u>

- **Overview:** Notices to Appear (NTA), otherwise known as I-862 forms, formally commence a proceeding in immigration court, and provide instructions to the noncitizen for when and where to appear before an immigration judge. These documents are typically initiated by a DHS component and are currently shared as paper files across CBP, ICE, USCIS, and DOJ. The electronic NTA sharing service enables agencies to digitally sign and exchange NTAs with those with a need to know, eliminating the need to manually print and fax documentation. This service will facilitate timely and secure exchange of NTAs and associated information to reduce human error or inaccuracies and limit the creation of duplicative forms as documents are exchanged across agencies.
- **Users:** CBP, DOJ, ICE, USCIS

6. <u>I-213 Service</u>

- **Overview:** The I-213 service allows signed I-213 forms and the data elements captured within the form to be accessed by interagency partners. I-213s originating with CBP, ICE, or other agencies involved in the immigration process are shared with other agencies as an individual moves through the immigration lifecycle. This service removes the need for I-213s to be distributed via mail, fax, or e-mail, and improves the security, speed, and transparency on data shared across partners.
- **Users:** CBP, DOJ, HHS, ICE, USCIS

7. <u>2500 and 2501 Service</u>

- **Overview**: The 2500 and 2501 Service facilitates the sharing of CBP Form-2500 and Form 2501 medical forms between USBP and OFO, allowing insight into a subject’s medical history. With the service, the most recent Form 2500/2501 created in Unified Secondary, E3, or EMR can be pulled back in another source system, allowing for officers, agents, and medical contractors to make medical care decisions based on more robust information.

- **Users**: CBP, ICE, HHS

8. <u>eSignature Service</u>

- **Overview**: The eSignatures Service provides both signed and unsigned immigration forms from USBP and OFO for a particular individual. The eSignature Service allows for users to view information before an individual physically enters their custody to better prepare for receiving individuals, which allows for more expedited processing and placement. Example forms include the I-862, I-286, and I-826.
- **Users**: CBP, ICE, HHS, USCIS

9. <u>Data Ingest Service</u>

- **Overview:** The Data Ingest Service allows agencies to access and receive data that the agency is unable obtain due to lack of an open connection. For example, the ICE Case Acceptance System (CAS) connects with the UIP via Databricks. This connection enables CBP to provide ICE with real-time notification upon completion of CBP's intake and processing, to enable ICE to initiate the case acceptance process. This service streamlines the manual process and significantly reduce the processing times.
- **Users:** CBP, ICE, USCIS

10. <u>Timeline as a Service</u>

- **Overview:** The Timeline as a Service gives agencies the ability to match an individual's major events and processing milestones from multiple sources on a single timeline, providing insight into that individual's end to end immigration journey.
- **Users:** CBP, ICE, HHS, USCIS, DOJ

11. <u>Manifest Service</u>

- **Overview:** The Manifest service allows for agencies to view an individual's transportation manifest electronically and eliminates the use of spreadsheets and manual emails created between CBP and ICE to coordinate individual transfers. The service eases the handoffs of the manifest between ERO officers and CBP agents and officers by allowing CBP and ICE to plan and make transportation arrangements regarding the individual electronically. This service also allows transportation arrangements to be shared in real-time with other parties, like HHS, who are currently notified via email.

- **Users:** CBP, ICE, HHS

12. A-file Service

- **Overview:** The A-file service allows for DHS user agencies to send forms data to the USCIS Content Management System, a backend repository of all digital immigration-related content. User agencies may access and retrieve these forms, through the CMS user interface called STACKS.[55]
- **Users:** CBP, ICE, USCIS

[55] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CONTENT MANAGEMENT SERVICE, DHS/USCIS/PIA-079, *available at* https://www.dhs.gov/privacy-documents-us-citizenship-immigration-services.