Privacy Impact Assessment
for the

CBP Enterprise Analytics

DHS/CBP/PIA-063

May 6, 2020

Contact Point
Rob McMullen, Executive Director
Border Enforcement Management Systems
Office of Information Technology
U.S. Customs and Border Protection
(571) 468-8200

Reviewing Official
Dena Kozanas
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

U.S. Customs and Border Protection (CBP) maintains large, unstructured, transactional databases to fulfill its various border security and law enforcements missions. To better understand and visualize patterns and anomalies within existing datasets, CBP is deploying Enterprise Analytics (a collection of information technologies and tools, known throughout this PIA as CBP EA) using internal datasets and other data sources available to CBP in support of its border security and law enforcement missions. These capabilities allow CBP to more effectively analyze and interpret existing data without changing or impacting the integrity of the data in the legacy source databases. CBP is publishing this Privacy Impact Assessment (PIA) to assess the privacy risks and mitigations for the use of these data aggregation analytic tools, which will extract and use existing personally identifiable information (PII) for data analytics and visualization.

Overview

As the nation's largest law enforcement agency, CBP is responsible for securing U.S. borders while facilitating lawful travel and trade. As part of CBP's authority to protect the border and enforce applicable laws at the border, CBP conducts research and analysis on its existing data systems to effectively visualize trends and patterns that could identify potential law enforcement or security risks. CBP EA provide CBP leadership and officers with mission critical capabilities that enable rapid analysis and visualization of CBP data in real-time to assist their decision-making processes.

CBP is deploying CBP EA to perform enhanced analysis of internal datasets and other data sources available to CBP in support of its border security and law enforcement missions. CBP EA assists CBP efforts by helping CBP personnel to use existing data more efficiently and effectively. CBP EA assists CBP and partner agency users in performing faster, more complete and complex data-driven analysis, often to inform executive leadership decision-making. CBP EA reduces the likelihood of human error by enabling automated analysis of several databases simultaneously, analysis that previously was performed serially and compared manually by analysts in the absence of the tools. CBP EA 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 a quantitative or statistical analysis). Lastly, CBP EA allows authorized users to structure the resulting information in a way that provides context and accurately interpret the data.

About CBP Enterprise Analytics

The CBP EA tools are not part of the underlying databases or source IT systems. They do not change any data in a source system or database or permanently retain data. Typically, CBP EA tools fall within the following four types:

- **Data Visualization Tools:** Data Visualization tools support the need to visualize enhanced data sets to depict complete transaction and entity lifecycles, and complex analytical output. Typically, the Data Visualization tools work in conjunction with the other tools below and provide a visual depiction (like a graph) of the outputs from these tools.
- **Search Tools:** A search tool is one that allows an analyst to quickly find information (e.g., allowing authorized users to query more than one data set simultaneously) or compare two data sets to which the analyst has access (e.g., comparing average Time in Custody rates for different migrant holding facilities).
- **Exploratory Analysis Tools:** Exploratory analysis tools assist a user in understanding more about the data, so that the user can determine the next steps he or she should take in the analysis. For example, exploratory analysis tools may provide the user with descriptive statistics (e.g., average, maximum, minimum, count, and odds ratio) or graphs (e.g., box plot, dot plot, and histogram). The goal of these tools is not to make conclusions, but to describe the data in a meaningful way that allows the analyst to interpret the data more efficiently. An example of an exploratory analysis tool would be one that tracks changes in average Time in Custody rates for different migrant holding facilities over a specific period of time.
- **Advanced Analysis Tools:** Advanced analysis tools assist a user in interpreting the data to answer management, operational, or intelligence questions. These tools could include inferential statistics (e.g., confidence intervals, hypothesis testing, classification, and regression), entity resolution algorithms, or other data modeling capabilities (e.g., network analysis, trend analysis, or geospatial analysis). An example of an advanced analysis tool would be one that plots increases in Time in Custody rates at migrant holding facilities on a map, allowing an analyst to view trends using geographic locations and determine how to best use available resources.

Compliance Framework

In an effort to be flexible in meeting mission needs while ensuring privacy compliance, CBP will deploy CBP EA tools consistent with this PIA. Prior to deployment of any new or proposed tools, CBP will conduct a Privacy Threshold Analysis (PTA) to determine whether additional compliance documentation is necessary, including updates to source system PIAs and System of Records Notices (SORNs). PTAs for proposed tools shall include information such as:

- A description of the tool's functionality;
- Type of analytical capabilities the tool provides (e.g., data visualization, search, exploratory analysis, advanced analysis, or multi-capability);

- The management, operational, or intelligence question or process challenge the tool is designed to address;
- The intended outcome (e.g., mission impact) for the mission requestor;
- The data that will be used or accessed;
- A list of the anticipated CBP organizations that would use the tool;
- Whether and what types of PII the tool will access;
- Whether the tool will generate or create new data;
- Where or how the data will be accessed, generated, created, or stored;
- Whether the tool accesses commercial or publicly available data;
- Whether the tool performs data mining;
- Whether the tool relies on or attempts to identify individual characteristics that are protected (e.g., nationality, gender), accesses categories of information with additional protections (e.g., asylum records), or implicates other individual rights; and
- What measures are in place to evaluate the tool's effectiveness.

With this detailed information, the CBP and DHS Privacy Offices will conduct a review the proposed tool via the PTA process.[1] If the tool is approved for coverage under this PIA, it will be added to the Appendices of this PIA.

PIA Structure

CBP is conducting this PIA to provide transparency and, using the DHS Fair Information Practice Principles, evaluate any privacy risks associated with CBP EA.[2]

This PIA describes the approved use cases for the CBP EA. All use cases are consistent with CBP border security and law enforcement authorities and conform to the purpose for which the data was originally collected. CBP EA tools enable users to look at trends and patterns in data that are critical to CBP operations. The automated nature of enhanced analytics increases the efficiency and effectiveness of CBP managers at all levels within the CBP organization to and allows them to easily identify mission critical information and discover trends and patterns in travel and trade behavior. At a high level, CBP anticipates using the EA tools to assess existing data for the following use cases:

[1] CBP Privacy Office requires business owners who deploy Enterprise Analytic tools to conduct a PTA describing the tool, type of technology, analysis to be performed, and expected outcome. The DHS Privacy Office adjudicates all PTAs.
[2] Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security.

1. Executive-level Decision-Making – CBP Executives are moving toward increasingly data-driven decision-making. Executives have a need to be able to assess and visualize data about their specific areas of responsibility to make fact-based leadership and management decisions.
2. Strategic Resource and Asset Allocation – CBP is responsible for securing and safeguarding vast amounts of information, locations, personnel, and resources. EA tools will give CBP field-level leadership a high-level view of whether assets are being over or underused, which will allow CBP to more effectively deploy its limited resources.
3. Custody and Apprehension Information Trends and Patterns – CBP and other Agencies involved in the immigration enforcement and custodial requirements for alien detention require better integration and faster, visual depictions of changes in patterns of apprehensions, extended or decreased time in custody, and amount/location of individuals in Federal administrative custody.
4. Immigration Process Flow Analysis – Better integration across CBP and other Agencies involved in lawful and unlawful immigration within the U.S. Government to create a full picture or timeline of an individual's consolidated interactions with the U.S. immigration system.
5. Trade Information Analytics – EA tools will provide data visualization to support the trade and cargo security missions within CBP by visualizing enhanced data sets to depict complete transaction and entity lifecycles, and by providing complex analytical output. EA tools support data driven decisions that discover emerging risks, new trade patterns, and allow CBP to assume a more proactive enforcement and risk-assessment posture.
6. *Law Enforcement Intelligence* – CBP's mission includes identifying potential law enforcement and security risks, and developing intelligence to counter those risks. EA tools will allow users to identify individuals, associations, relationships, or patterns that may pose a potential law enforcement or security risk, and assist users in the field in preventing violations of law or regulations at and/or between ports of entry.

Appendix A offers a detailed description of the functionality of each CBP EA tool. The CBP Privacy Office maintains a full list of approved use cases and source data sets for each tool. The use of the source system data within the analytical tools results in the generation of work products. These types of outputs can include, for example, geospatial, temporal, hierarchical, multi-dimensional, and network visualizations, such as thematic-type maps connecting a specific theme to a geographic area, timelines, arc diagrams, histograms, bar charts, node-link diagrams, dashboards with multiple views of data, summaries of key statistics, trends, and other types of reporting work products. As was the case prior to the creation of the CBP EA compliance

framework, if the analysis creates any new Privacy Act records, the new work product records must be part of a system of records with notice provided in a SORN. The CBP Privacy Office identifies the applicable SORN for such work products, or determines that a new SORN is needed, as part of the PTA process.

Appendix B details the data approved for use by the CBP EA tools. CBP EA tools do not grant new access to raw data to users or allow a user to view underlying system data he or she has not already received permission to view. Rather, CBP EA tools display read-only data from either a data warehouse (e.g., Enterprise Management Information System-Enterprise Data Warehouse (EMIS-EDW))[3] containing data from the underlying source systems, or from a local copy of the source system data housed within the tool that updates at an agreed upon refreshed time rate.[4] At no point can any CBP EA tools make any changes to a source database. Users cannot change or manipulate the underlying data via the tools. Appendix B details the applicable System of Records Notices (SORN) and Privacy Impact Assessments (PIA) that govern the underlying source datasets. The Appendix also includes information about the databases that may impact the quality or integrity of the source system data, such as the platform's refresh rates from the source system.

CBP will update the Appendices as the new tools and use cases are approved.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[5] articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[6]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[7] The FIPPs account for the

---

[3] DHS/CBP/PIA-034 Enterprise Management Information System-Enterprise Data Warehouse (EMIS-EDW) (September 7, 2016), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp_emis_edw-appendixd-april2019.pdf.

[4] CBP EA tools will access underlying source data either directly from the source system itself, or to ease the strain on the live transactional databases will access the source system data through aggregated enterprise databases and data warehouses.

5 5 U.S.C. § 552a.

6 6 U.S.C. § 142(a)(2).

7 See Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security," available at www.dhs.gov/privacy.

nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208[8] and the Homeland Security Act of 2002 Section 222.[9] Given that CBP deployment and oversight of CBP EA are multiple privacy sensitive technologies deployed on existing CBP datasets, CBP is conducting this PIA as it relates to the DHS Fair Information Practice Principles.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate.

CBP users and executives (and in some cases, approved DHS or other agency partners) use EA tools for a variety of approved uses, typically to make data-driven decisions about resource or asset allocation. The analytic tools do not collect information directly from the public; however, the underlying source data systems often contain information collected directly from an individual. To provide transparency to the public about these analytic tools, CBP is publishing this high-level PIA to describe the specific data sets, databases, and types of CBP EA tools deployed. Appendix B provides detailed information about data sources for which DHS previously provided notice related to the collection and use of information through Privacy Act Statements[10] (as applicable) and its publication of SORNs and PIAs.[11] Appendix B includes information for the data sets and databases, including data set name, description, relevant compliance documents, populations covered, data elements covered, data retention requirements, and data refresh rates from the source system. CBP will update Appendix B as additional datasets are approved for advanced analytics.

CBP EA tools' access and use of source data does not change the circumstances of or purpose for the original information collection. The CBP EA tools provide new technical capabilities to support CBP's existing use and understanding of its information, and do not change the purpose for which CBP uses the information.

---

8 44 U.S.C. § 3501 note.
9 6 U.S.C. § 142.
[10] Pursuant to 5 U.S.C. § 552a(e)(3) agencies are required to provide what is commonly referred to as a Privacy Act Statement to all persons asked to provide personal information about themselves if that information will go into a system of records (i.e., the information will be stored and retrieved using the individual's name or other personal identifier such as a Social Security number).
[11] All DHS SORNs and PIAs are available on the DHS Privacy Office website at www.dhs.gov/privacy.

Privacy Risk: There is a risk that individuals will not be aware that CBP is using advanced analytics tools to process their information.

Mitigation: This risk is mitigated. CBP is providing notice of CBP EA through the publication of this overarching PIA. In addition, as part of the PTA review process, when CBP considers additional source data for use by advanced analytic tools, CBP will determine specifically whether additional notice at the point of collection is needed given the contemplated uses of the data or source IT system. CBP will also determine whether the PIAs and SORN for the source IT systems need to be updated to provide additional transparency.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

The CBP EA tools use existing data sets and data sources and do not collect information directly from individuals or change the initial collection of the information taking place at the source system. Depending on the source system, notice may have been provided by Privacy Act Statements or applicable SORNs and PIAs.

Many of the datasets accessed by the CBP EA tools originally collected information directly from a record subject. Depending on the source system, individuals may have had the opportunity to consent, decline, or opt out at the time the information was collected. There may be instances when the CBP EA tools draw information from law enforcement systems that maintain information about individuals that is not collected directly from the individuals (e.g., information from an encounter with an individual or information from a witness or victim about a suspect). These individuals do not have an opportunity to decline to provide the required information, opt out, or to consent to uses.

CBP's use of CBP EA will not impact the individual's ability to access and correct his or her information consistent with the published SORN for the source systems.

Privacy Risk: There is a risk to individual participation because individuals do not have the opportunity to consent to their information used by CBP EA tools.

Mitigation: This risk is partially mitigated. CBP EA tools do not collect information directly from an individual. However, CBP mitigates this risk by ensuring that CBP EA tools cannot change or modify the underlying source system records, to which CBP continues to provide access, correction, and redress. These source systems, to the extent permitted by law, offer

individuals the opportunity to provide their information directly to CBP and often provide notice at the time of collection.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

CBP collects information which may be subject to further analysis in support of agency activities based on numerous authorities, including Title II of the Homeland Security Act of 2002 (Pub. L. 107-296), as amended by the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108-458, 118 Stat. 3638); the Tariff Act of 1930, as amended; the Immigration and Nationality Act ("INA"), codified at 8 U.S.C. § 1101, et seq.; the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110-53); 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); Aviation and Transportation Security Act of 2001 (Pub. L. 107-71); and 6 U.S.C. § 202. CBP develops EA tools for purposes that support existing law enforcement and border security authorities. The EA governance structure allows CBP to ensure that CBP is using the information consistent with its authorities and with the original purpose of the collection.

Privacy Risk: There is a risk that CBP does not specifically articulate the use of information for analytical purposes at the time of collection.

Mitigation: This risk is mitigated. CBP ensures that CBP EA tools described in this PIA use existing CBP data consistent with the original purpose of the collection. PTAs are developed for all tools being considered to be included as part of this PIA, and the PTA will include a discussion of the data sets involved. If the analysis concludes that the purposes articulated at the time of collection is not aligned, the tool may not be eligible to be included as part of this PIA and would require its own PIA to assess the risks associated with the proposed use of CBP data.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

CBP EA tools do not collect any additional information from individuals; the tools access only existing data from source systems. The tools either extract and maintain from the source system a temporary local copy of the data within the tool or on a local, secure network drive, or the tools access the data directly from a data warehouse. For most situations, CBP EA tool

operators and the CBP Privacy Office will collaboratively review proposed refresh rates and retention limitation, in order to assess the degree of acceptable risk and determine necessary mitigations. Generally, CBP EA tools do not retain obsolete data since the tools are refreshed by a source system or database. However, there are cases where data accessed from the source systems is internally "cached" (i.e., temporarily stored) in order to be processed by the CBP EA tool for further analysis. Cached data is purged at the end of users' session or when the user closes the application. If, by exception, there is a need for the CBP EA tool to retain the static data beyond the duration of a session, the data will be retained consistent with the source system retention schedules.

In cases in which a user chooses to retain the results of the analysis, the retention must be consistent with the applicable SORN for the work product. During the PTA review process the CBP Privacy Office will recommend the applicable SORN to the DHS Privacy Office and identify a schedule that covers the retention of any results. The CBP Privacy Office will document the SORN in the written tool summary. Typically, users maintain the output of the tools (such as electronic results or written analysis) in a shared space (e.g., access-controlled SharePoint sites) in which users may collaborate with other users. This storage of results must also be consistent with the SORN that covers the user's analytical results.

Privacy Risk: There is a risk that CBP program offices will store local copies of the extracted data prior to upload into the tool for unknown periods of time.

Mitigation: This risk is partially mitigated. As part of the PTA process, CBP Privacy Office staff counsel and advise programmatic offices on the method and duration that data extracts from the source systems may be stored. All data extracts must be stored in a secure location on the CBP intranet, and anyone with access to the storage location must have a valid CBP background investigation and a need to know. Typically, this means an access-controlled folder or partitioned section of a local shared drive. CBP Privacy Office advises that local copies of the extracts be deleted once the analysis is complete, or once the program office has created merged files to anonymize the information and no longer needs the raw extraction files.

Privacy Risk: There is a risk that CBP EA tools will retain data for longer than is necessary, or for a longer period than allowable under the source system retention schedule.

Mitigation: This risk is partially mitigated. CBP EA tools do not generally retain un-refreshed data past the end of the users' session. It is possible for users to save their own session with un-refreshed data; however, there is no useful purpose for this and would only be available to the single user who saved the un-refreshed data.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

CBP EA tools are deployed to perform enhanced analysis of internal datasets and other data sources available to CBP in support of its border security and law enforcement missions. These advanced analytic tools assist CBP efforts by helping CBP personnel to use the data they already have more efficiently and effectively. The CBP EA tools are not part of the underlying databases or source IT systems. They do not change any data in a source system or database or permanently retain data.

CBP EA tools enable users to look at trends and patterns in data that are critical to CBP operations. The automated nature of enhanced analytics increases the efficiency and effectiveness of CBP managers at all levels within the CBP organization to easily identify mission critical information and discover trends and patterns in travel and trade behavior.

At a high level, CBP anticipates using the EA tools to assess existing data for the following purposes:

1. *Executive-level Decision-Making* – CBP Executives are moving toward increasingly data-driven decision-making. Executives have a need to be able to assess and visualize data about their specific areas of responsibility to make fact-based leadership and management decisions.
2. *Strategic Resource and Asset Allocation* – CBP is responsible for securing and safeguarding vast amounts of information, locations, personnel, and resources. EA tools will give a high-level view of whether assets are being over or underused, to allow CBP to more effectively deploy its limited resources.
3. *Custody and Apprehension Information Trends and Patterns* – CBP and other Agencies involved in the immigration enforcement and custodial requirements for alien detention require better integration and faster, visual depictions of changes in patterns of apprehensions, extended or decreased time in custody, and amount/location of individuals in Federal administrative custody.
4. *Immigration Process Flow Analysis* – Better integration across CBP and other agencies involved in lawful and unlawful immigration within the U.S. Government to create a full picture or timeline of an individual's consolidated interactions with the U.S. immigration system.
5. *Trade Information Analytics* – EA tools will provide data visualization to support the trade and cargo security missions within CBP to visualize enhanced data sets to depict

complete transaction and entity lifecycles, and complex analytical output. EA tools support data driven decisions that discover emerging risks, new trade patterns, and allow CBP to assume a more proactive enforcement and risk-assessment posture.

6. *Law Enforcement Intelligence* – CBP's mission includes identifying potential law enforcement and security risks, and developing intelligence to counter those risks. EA tools will allow users to identify individuals, associations, relationships, or patterns that may pose a potential law enforcement or security risk, and assist users in the field in preventing violations of law or regulations at and/or between ports of entry.

Typically, most CBP EA tools generate an output that is stripped of any personally identification information. The tools are used to generate charts or graphs to show patterns and analysis of the raw data used to generate the analytic outputs. CBP will share these products with external partners consistent with the underlying source system data and consistent with applicable information sharing access agreements (ISAA). To the extent the information in the analytic products contain PII, then CBP will only share consistent with the relevant SORNs governing the source system information and need to know requirements.

Privacy Risk: There is a risk that CBP's use of CBP EA on existing data may be inconsistent with the original purpose of collection.

Mitigation: This risk is mitigated. The authorized use of a particular data set is described in the SORN and PIA for that data or program, and CBP EA may only use data consistent with the SORN and PIA for a particular data set. CBP EA does not provide a user with any access to DHS data that CBP has not already provided public notice about through an associated SORN and/or PIA. Furthermore, all policy and legal controls that apply to a particular data set are adhered to when the data is used. CBP will conduct PTAs for all CBP EA tools being considered for inclusion under this PIA. If the PTA analysis concludes that the use considered is not consistent with the original purpose of collection, the tool may not be eligible to be included as part of the CBP EA compliance framework and would require its own PIA to assess the risks associated with use limitation.

Privacy Risk: There is a risk that CBP EA tools may access and make available data that is subject to confidentiality provisions and cannot be shared with external partners.

Mitigation: This risk is mitigated. For the most part, CBP EA tools will generate an output that is not privacy sensitive—such as graph or chart of activity in a certain location. To the extent an output generated by the CBP EA tools includes PII, CBP will not disclose to third parties information contained in or pertaining to any asylum application, records pertaining to credible

fear determinations, or the fact that a particular individual has applied for asylum or received a credible fear or reasonable fear interview.[12]

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

To ensure the accuracy and integrity of data, CBP EA tools will access data from the source systems or established CBP data aggregators such as EMIS-EDW, which obtains its data from the source systems. CBP EA tools do 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. EA tools allow users to make decisions based on source data; therefore, data is verified with source systems to ensure data accuracy. In cases where a CBP EA tool extracts and maintains a temporary local copy of the data, the operators and the CBP Privacy Office will collaboratively review the proposed refresh rate and assess the degree of acceptable risk in order to determine appropriate mitigations, if any. The proposed refresh rates will provide the maximum assurance possible that data is accurate, relevant, timely, and complete. Users only access tools for which they received training on the underlying source to understand the risks associated with the data latency and data verification.

Privacy Risk: There is a risk that CBP EA tools will make operational determinations about individuals using stale or inaccurate information.

Mitigation: The risk is mitigated. CBP EA tools provide information used for managerial, strategic, research, and intelligence purposes; the tools do not make any operational determinations about individuals. The tools are not creating any original work product; rather it is replicating the creation of already approved work product more efficiently for tool users. For example, a supervisor at a detention facility may use a tool to more quickly analyze processing wait times for individuals within the facility. The tool itself will not make processing order determinations, but will provide information to the supervisor who can then use the information to make decisions about how to manage resources to improve processing efficiency at a facility. As indicated in each respective PTA for the tool and use case, the data within each tool is refreshed regularly to prevent the use of stale or inaccurate information.

While CBP EA tools facilitate analysis of existing CBP data, any decision impacting an individual (as opposed to a managerial decision about overall resource or asset allocation) is based on the source system data, to which existing access, redress and correction procedures still apply.

[12] 8 CFR 208.6.

Furthermore, CBP EA tool users only access tools for which they have received permission to view and use the underlying system data. Users must provide a certificate verifying underlying system training certification before receiving access to the underlying system. Training for the underlying systems includes training regarding the risks associated with data latency and data verification. Validation processes will be reinforced by integrating features within the tools to validate critical data elements against the source systems from the CBP EA tools. CBP minimizes data latency to the greatest extent possible to ensure that CBP EA tools rely on the most accurate and up-to-date data available from the source system.

Privacy Risk: There is a risk that information within CBP EA may be outdated or inaccurate because some CBP EA tools extract and maintain a temporary local copy of the data from the source systems.

Mitigation: This risk is mitigated. In most cases, CBP EA tools rely upon the source systems to ensure data quality and integrity. In cases in which a tool extracts and maintains a temporary local copy of the data from the source systems, an acceptable data refresh rate will be defined based on the assessment by the CBP Privacy Office. Additional measures that enable users to validate quality and integrity of the data will be developed and integrated into the tool as a feature.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

CBP is following the requirements for information assurance and security for the CBP EA data sets, databases, and tools. They either have undergone, are undergoing, or will undergo the DHS security review process 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 will be included in a security Authority to Test (ATT) package for review and approval by the Chief Information Security Officer (CISO) or Interim-Authority to Operate (I-ATO) package prior to the tools storing or using any data. ATTs or I-ATOs are valid for six months. Within that six months, the use case, tools, and data must either be decommissioned or validated using the full security authorization process for an Authority to Operate (ATO). Many of the tools contemplated fall under the existing security authorization for "Data Cube Enterprise Analytics," which was accredited on May 2, 2019.

CBP EA tool users will only be able to access data for which they have received authorization. In other words, EA tool users must be separately authorized to access the underlying source system data in order to access that data within the tool. Should new access to data 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. Appendix A provides information on the approved mission uses cases. All users have read-only access and cannot change the underlying data. Data extracted from a system and uploaded into the tool will only be visible to the single user who uploads the data; other users will not have access to that data. Users are able to share or publish tool products to a page that other users can access; however, those users can only access and view the shared or published pages if they themselves have approval to view the underlying source system data.

Privacy Risk: There is a risk that individuals who are not authorized to access source system data will be granted access to data contained in CBP EA tools.

Mitigation: This risk is mitigated. To mitigate this risk, CBP will detail its intended user group and their authority to access related underlying data within the PTA. In addition, the user approval process and access roles will be described within the privacy documents of the underlying systems to ensure users are only granted access to information necessary to perform their official duties. All CBP EA users complete annual mandatory privacy and security training, which stresses the importance of appropriate and authorized use of personal data in government systems.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

CBP EA tools 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 Office offers role-based training for agency employees involved with information sharing.

CBP EA tools use audit logging so that user requests and the results returned 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.

Privacy Risk: There is a risk that individuals who are not authorized to access source system data will be granted access to data contained in CBP EA tools.

Mitigation: This risk is mitigated. CBP ensures that privileged user access is tightly

controlled by the CBP Amazon Web Service Cloud Environment (CACE) team and database teams. In order to access the servers that store and process data, a user must be approved by the source system owner, who validates authorization, and the CACE administrators, who validate that users only access approved systems. These systems are accessed using validated, logged, and Identity, Credential, and Access Management (ICAM) controlled credentials. These are all inherited controls that come from ICAM. None of these systems use passwords, only government-issued Personal Identity Verification (PIV) cards with accompanying PIN.

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, under the normal course of how the authentication system works, to validate whether the individual requesting access is authorized to access the system.

Responsible Officials

Rob McMullen
Executive Director
Border Enforcement and Management Systems Program Directorate (BEMSD)
Office of Information Technology
U.S. Customs and Border Protection
(571) 468-8200

Debra L. Danisek
CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection
(202) 344-1610

Approval Signature

[Original signed and on file with the DHS Privacy Office]

_____

Dena Kozanas
Chief Privacy Officer
Department of Homeland Security

Appendix A: Approved Enterprise Analytics Tools

Last Updated: May 10, 2022

1. Athena/Data Cube

Athena uses Data Cube, a Commercial off-the-Shelf (COTS) business intelligence and data analytics tool that integrates CBP and other Federal agency data sources. Athena enables users to readily track and report on the movements of individual migrants and migrant groups as they are processed and transferred between government facilities and stakeholders. Athena facilitates collaboration between CBP and ICE to evaluate, monitor, and respond to current issues in migrant processing.

Athena uses the following data sources:

- Enterprise Management Information System - Enterprise Data Warehouse (EMIS-EDW) (which aggregates data from various source systems, listed below)
- Department of Health & Human Services Unaccompanied Alien Children Data (HHS UAC). Individual Athena users who are authorized to access HHS UAC data will upload a file to Athena via the browser during their session.

Athena has access to the following data sources within EMIS-EDW:

- Seized Currency and Asset Tracking System (SEACATS)
- Enforcement Case Tracking System (E3/ENFORCE)

Athena does not retain source system information beyond what is displayed during a user session. Athena captures and visualizes a migrant's journey while in custody in one view; provides a dashboard that identifies current pain points in migrant processing; provides a dashboard that identifies communities and individuals with longer than acceptable Time in Custody (TIC); and presents information in an interactive timeline and geo-spatial views.

2. Qlik

Qlik is a COTS business intelligence and data analytics product that integrates data from multiple sources. Qlik provides a dashboard functionality with visualization and reporting capabilities that facilitate the exchange of information and intelligence. This automated visualization technology saves CBP personnel resources and reduces the time and effort spent compiling statistics and analytics to support mission critical decisions and responses to inquiries.

Like most CBP EA tools, Qlik captures and visualizes data through customizable

dashboards, provides a graphical representation of data where the individual values contained in a matrix are represented as colors helping to drive priority and focus of operations, presents high-level information for decision makers in a graphical timeline and interactive geo-spatial views, and identifies and analyzes causes of data changes.

3. PowerBI

PowerBI is an interactive data visualization reporting tool that lets CBP users import, manipulate, visualize, and analyze their own data. The software is scalable, allowing CBP personnel at all levels to analyze and visualize different aspects of the same data in one place, and create dashboards and reports to quickly monitor and drill down into their most important information without the help of OIT. The ability to unlock data, transform it into actionable insights, and share it in new ways enables CBP teams to improve services and increase responsiveness to mission needs.

Any CBP employee on a CBP workstation can access the software center and install PowerBI desktop; the tool is free and doesn't require a license. However, the CBP Privacy Office requires that users conduct a Privacy Threshold Analysis if extracting data for use in PowerBI. PowerBI can ingest and process excel files, oracle databases, business objects, Salesforce data, SharePoint lists and libraries, and shared drives. CBP users can point the tool towards these files if saved on a local network drive and it can compare and contrast the information contained within the files. PowerBI can connect to hundreds of data sources and refresh them within the software desktop once they are connected.

Once imported, data can be shaped and transformed. PowerBI can rename, edit, and merge data in bulk, and can save processes previously applied to data as "steps" so the user can refresh and update data more efficiently. PowerBI also recognizes underlying associations within data sets and creates relationships and connections automatically upon import. These relationships can become visualizations by drag-and-dropping them onto the dashboard canvas. If the default visualizations are insufficient, Microsoft and partners have hundreds of visualization templates that can be adjusted to the dashboard's needs. Dashboards are interactive, and selecting a particular facet of the data can bring up more information and adjust measures on the dashboard in real time.

PowerBI lets any CBP user dig deep into the data using features like quick measures, grouping, forecasting, and clustering to explore and discover. The query system is also intuitive for entry-level users, relying on natural language for quick discovery. After building, a user can share their work by exporting their dashboard through creating a PDF, emailing it to another PowerBI user, or, given a license from OIT, embedding it within a website.

PowerBI is used across CBP for any of the approved use cases noted in this PIA. CBP Privacy Office maintains an inventory of all approved PowerBI use cases with an approved PTA on file.

4. Databricks

Databricks is an analytics platform application optimized to run on the CBP Amazon Web Services (AWS) Cloud East (CACE) cloud services platform. Databricks allows CBP to build data pipelines and provide a platform to support business intelligence (BI) reporting and execution of advanced capabilities, such as data mining, and machine learning. With Databricks, data in any form (raw or structured) can be streamed or processed in batches and ingested into the AWS CACE platform. The data can then be accessed, transformed, and organized by Databricks for specific analytical use cases. Once processed, end users can access Databricks through a web interface. CBP uses Databricks as a data lake to store existing datasets to analyze the data for various use cases including reports, dashboards, and advanced analytics.

Databricks allows users to produce reports and analytics, which may include calculating statistical measures. Information will be de-identified based on the mission use case, audience, and need to know. In most cases, reporting will be aggregated and will not include subject level data unless required by the mission. Currently, Databricks is used by CBP, ICE, and DHS HQ for any of the approved use cases noted in this PIA. If CBP provides access to Databricks beyond CBP, ICE, and DHS HQ, CBP will update this appendix to reflect additional users. The CBP Privacy Office maintains an inventory of all approved Databricks use cases with an approved PTA on file. The below systems are a list of the data sources that are ingested into Databricks. All data sources are outlined in greater detail in the approved Databricks PTA.

DHS Datasets:

- **E3/Enforcement Integrated Database (EID):**[13] Databricks accesses all EID data points within the e3, except for biometric images. To ensure data remains current and accurate, Databricks connects to e3/EID in near real-time. This helps further reduce the latency that exists within the reporting and BI tools in use and provides CBP users and leadership accurate and up-to-date information.
- **Immigration Integrated Decision Support/Bond Management Information System (IIDS/BMIS):**[14] This system enables ICE Office of Enforcement and Removal Operations (ERO) users to analyze the data from the data warehouse using pre-defined

[13] *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.
[14] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE BOND MANAGEMENT INFORMATION SYSTEM, DHS/ICE/PIA-005, available at https://www.dhs.gov/privacydocuments-ice.

and ad-hoc queries and allows ERO to report on a variety of immigration enforcement activities including encounters, arrests, bonds, detainers, detentions, and criminal and removal cases. ERO personnel use IIDS to run reports both at the aggregate and individual levels. ERO personnel also use IIDS to receive information and search individual records by personal identifier, although this use is less frequent than running statistical and aggregate reports. Databricks takes in all IIDS fields that are available in BMIS and EID.

- **ICE ServiceNOW (SNOW):**[15] The ServiceNOW (SNOW) Bed Request System (BRS) and the Arrest Approval Reporting Worksheet (AART) are onboarded into Databricks for use by ICE and CBP to aid efficiency in resource availability and to obtain approval for certain enforcement actions.
- **Tasking, Operations, and Management Information System (TOMIS):**[16] TOMIS is a unified data processing and reporting environment for CBP aviation and maritime field operators. Databricks accesses all TOMIS data with the exception of user account information. Similar to e3/EID, Databricks connects to TOMIS in near real-time, ensuring a reduction in the latency that exists within the reporting and BI tools in use.
- **Team Awareness Kit (TAK):**[17] TAK is a suite of government off-the-shelf software (GOTS) that allows mobile device users to send their location and receive the locations of teammates connected to the same TAK Server. Users can also chat and send pictures and receive mission packs. CBP is ingesting TAK data within Databricks for easier access to the data for use by the TAK team only.
- **HRM Consolidated Analytics Platform (HCAP):**[18] Databricks will store data for reporting and analysis across CBP Human Resources (HRM). HRM uses the employee HR data to build data pipelines, perform transformations, and provide a platform to support Business Intelligence (BI) reporting and execution of advanced capabilities.

---

[15] *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/privacydocuments-ice.
[16] TOMIS is a privacy-sensitive system that only collects information on CBP employees. Therefore, no PIA is required.
[17] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR TEAM AWARENESS KIT, DHS/ALL/PIA-090, *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.
[18] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE DHS TALENT ACQUISITION, DHS/ALL/PIA-043(a); U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE HUMAN RESOURCES BUSINESS ENGINE, DHS/CBP/PIA-032 HUMAN RESOURCES BUSINESS ENGINE, *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

- **DHS HQ Neptune:**[19] Databricks ingests detention facility address and location information for use within UIP. No PII is included in the data. Neptune is the vehicle for transmitting the data from DHS Immigration Data Integration Initiative (IDII), ensuring this is the most accurate detention location information.

External Datasets

- **Health and Human Services Unaccompanied Children Portal (HHS UC Portal):**[20] This portal shares only summary statistics with Databricks, which does not include PII. The statistics are limited to total number in Office of Refugee Resettlement (ORR) care, general shelter/capacity information, number of discharges, sponsor categorization, average length of care, and UC designations. The HHS UC Portal sends the data to an S3 bucket that connects to Databricks. This enables for better preparation for intake purposes and improved resource allocation across all government stakeholders.

[19] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE DATA FRAMEWORK, DHS/ALL/PIA-046, *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.
[20] *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.

Appendix B: Approved Datasets

Last Updated: May 6, 2020

Appendix B includes details and information on approved datasets that will be accessed by the various CBP EA tools.

A. CBP Sources/Systems

1. CBP Automated Commercial Environment

The Automated Commercial Environment (ACE) is the backbone of the U.S. Customs and Border Protection's (CBP) trade information processing and risk management activities and is the key to implementing many of the agency's trade transformation initiatives. ACE allows efficient facilitation of imports and exports and serves as the primary system used by U.S. Government agencies to process cargo. ACE collects information about individuals, companies, and government employees involved in commercial border transactions. This includes: truck carrier information; broker account information; importer account information; U.S. Postal information on importations; CBP and Participating Government Agency (PGA) employee information; and E-Manifest information which consists of specific details regarding the trip, conveyance, equipment, crew, and shipments related to a commercial land border crossing.

- PIA: DHS/CBP/PIA-003(b) Automated Commercial Environment (ACE), July 31, 2015 - Appendix Update March 2018[21]
- Associated SORN(s): DHS/CBP-001 Import Information System[22]

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

CBP's Seized Assets and Case Tracking System (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

[21] DHS/CBP/PIA-003(b) Automated Commercial Environment (ACE), *available at* www.dhs.gov/privacy.
[22] DHS/CBP-001 Import Information System, 81 FR 48826 (July 26, 2016).

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[23]
- Associated SORN(s): DHS/CBP-013 Seized Assets and Case Tracking System[24]

3. CBP Portal (E3) to ENFORCE/IDENT

CBP uses the e3 portal (e3) to collect and transmit data to ICE's Enforcement Integrated Database (EID) [25] and DHS's Automated Biometric Identification System (IDENT) [26] 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 the individuals they encounter by capturing the apprehended individual's photograph and fingerprints and transmitting them in real-time to IDENT; facilitate the capture and recording of data pertaining to border violence and alien smugglers; view and record information pertaining to criminal trials; build cases for prosecution; generate documents electronically per the requirements of a particular court; print, update, and track cases; and create statistical reports.

- PIAs
  - DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT[27]
  - DHS/ICE/PIA-015 Enforcement Integrated Database (EID)[28]
  - DHS/OBIM/PIA-002 IDENT[29]

---

[23] DHS/CBP/PIA-040 Seized Assets and Case Tracking System, *available at* www.dhs.gov/privacy.
[24] DHS/CBP-013 Seized Assets and Case Tracking System, 73 FR 77764 (December 19, 2008).
[25] *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID) and associated updates, *available at* www.dhs.gov/privacy, and DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 FR 72080 (October 19, 2016).
[26] *See* DHS/OBIM/PIA-002 Automated Biometric Identification System, *available at* www.dhs.gov/privacy. DHS is retiring IDENT and replacing it with the Homeland Advanced Recognition Technology System (HART), which will be discussed in a forthcoming PIA.
[27] DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT, *available at* www.dhs.gov/privacy.
[28] DHS/ICE/PIA-015 Enforcement Integrated Database (EID), *available at* www.dhs.gov/privacy.
[29] DHS/NPPD/PIA-002 IDENT, *available at* www.dhs.gov/privacy.

- Associated SORN(s)
    - DHS/CBP-023 Border Patrol Enforcement Records System of Records (BPER)[30]
    - DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records October[31]

4. CBP TOMIS (Tasking, Operations and Management Information System)

The TOMIS (Tasking, Operations and Management Information System) application is a web-based task and operations management system designed to provide consistent and standardized mission and case tracking and reporting services to Air & Marine Operations (AMO). TOMIS is a unified data processing and reporting environment for AMO operations, and is designed to be a robust, secure, and scalable system to facilitate important information transfers vital to the law enforcement mission. The core function of TOMIS is to provide a single tool for AMO aviation and maritime field operatives to schedule and process detailed pre- and post-mission data, process enforcement and non-enforcement events, perform mission functions related to aviation and maritime asset management, automate AMO subject targeting, and interface seamlessly with other in-house and external agency information technology products and initiatives.

- PIA: TOMIS does not store any information from members of the public, therefore it has no PIA.
- Associated SORN(s):
    - DHS/ALL-004 General Information Technology Access Account Records System of Records System (GITAARS)[32]
    - DHS/ALL-032 Official Passport Application and Maintenance Records[33]

5. CBP Border Protection Enforcement Tracking System (BPETS)

The Border Protection Enforcement Tracking System (BPETS) is an operational workforce management system designed to provide a single, standardized format for reporting within the U.S. Border Patrol (USBP). BPETS2 is an enhancement of the legacy BPETS system, and adds

[30] DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 FR 72601 (October 20, 2016).
[31] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 FR 72080 (October 19, 2016).
[32] DHS/ALL-004 General Information Technology Access Account Records, 77 FR 70792 (November 27, 2012).
[33] DHS/ALL-032 Official Passport Application and Maintenance Records, 76 FR 8755 (February 15, 2011).

advanced technologies and improved system integration. BPETS/BPETS2 contains multiple modules to track and manage the deployment of USBP personnel and operational assets; to analyze enforcement incident data (such as apprehensions and seizures); to create and approve operational orders; and to generate reports and statistics to ensure that USBP is efficiently deploying resources to meet enforcement needs along the U.S. borders. BPETS/BPETS2 maintains employee information such as personnel and medical records, employee time and attendance records, limited emergency contact information for USBP employees, and limited biographical and incident information for subjects of enforcement actions.

- PIA: DHS/CBP/PIA-046 Border Patrol Enforcement Tracking System (BPETS/BPETS2)[34]
- Associated SORN(s):
  - OPM/GOVT-1 General Personnel Records[35]
  - OPM/GOVT-10 Employee Medical File System Records[36]
  - DHS/ALL-014 Personnel Emergency Contact Information System of Records[37]
  - DHS/ALL-019 Payroll, Personnel, and Time and Attendance Records System of Records[38]
  - DHS/CBP-023 Border Patrol Enforcement Records (BPER)[39]

6. Air and Marine Operations Surveillance System (AMOSS)

The Air and Marine Operations Surveillance System (AMOSS) is the technical backbone for the Air and Marine Operations Center (AMOC), and CBP's common operating picture for air domain awareness. AMOSS is a sophisticated radar processing system that supports the concerted and cooperative effort of air, land, and sea vehicles; field offices; and command and control centers staffed by law enforcement officers (LEO), detection enforcement officers (DEO), pilots, crew, and AMOC support staff in monitoring approaches to the U.S. border to detect illicit trafficking and direct interdiction actions, as appropriate. Data will include blue force asset tracking information. AMOSS data will not contribute PII for CBP EA tools. Rather, it will provide AMO stakeholders with a comprehensive understanding of how and where AMO assets are used.

---

[34] DHS/CBP/PIA-046 Border Patrol Enforcement Tracking System (BPETS/BPETS2) (August 2017), *available at* www.dhs.gov/privacy.
[35] OPM/GOVT-1 General Personnel Records, 77 FR 73694 (December 11, 2012).
[36] OPM/GOVT-10 Employee Medical File System Records, 75 FR 35099 (June 21, 2010).
[37] DHS/ALL-014 Personnel Emergency Contact Information System of Records, 81 FR 48832 (August 25, 2016).
[38] DHS/ALL-019 Payroll, Personnel, and Time and Attendance Records, 80 FR 58283 (September 28, 2015).
[39] DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 FR 72601 (October 20, 2016).

- PIA: DHS/CBP/PIA-019 Air and Marine Operations Surveillance System[40]
- Associated SORN(s): DHS/CBP-019 AMOSS System of Records Notice[41]

7. Customs Automated Maintenance Inventory Tracking System (CAMITS)

The Customs Automated Maintenance Inventory Tracking System (CAMITS) is a web-based maintenance logistics system used by maintenance contractors to track the maintenance lifecycle of vessels and aircraft. CAMITS feature modules are related to: parts; assets; repairs; vehicles; financial; and reports.

- PIA: DHS/ALL/PIA-006 DHS General Contacts List[42]
- Associated SORN(s): DHS/ALL-004 General Information Technology Access Account Records System of Records System (GITAARS)[43] however CAMITS will not contribute any PII to support CBP EA.

8. Air and Marine Fleet Aircraft Management System (AMFAMS)

The Air and Marine Fleet Aircraft Management System (AMFAMS) is a tool for tracking information related to aircraft and associate support equipment and parts. It is used to track aircraft, equipment, inventory, maintenance, preventive maintenance, financial data, etc.

- PIA: AMFAMS collects information from CBP employees and contractors but does not store any information from members of the public, therefore it has no PIA.
- Associated SORN(s): DHS/ALL-004 General Information Technology Access Account Records System of Records System (GITAARS)[44] however AMFAMS will not contribute any PII to support CBP EA.

9. Operation Safety Standards Training Administration Resources (OpSTAR)

The Operation Safety Standards Training Administration Resources (OpSTAR) Portal is used to control access to and record usage of automated tests, web-based trainings, registration, transcripts, certifications, usage reports, and administrative functions of CBP employees and contractors.

---

[40] DHS/CBP/PIA-019 Air and Marine Operations Surveillance System, *available at* www.dhs.gov/privacy.
[41] DHS/CBP-019 AMOSS System of Records Notice 78 FR 57402 (September 18, 2013).
[42] DHS/ALL/PIA-006 DHS General Contacts List, *available at* www.dhs.gov/privacy.
[43] DHS/ALL-004 General Information Technology Access Account Records, 77 FR 70792 (November 27, 2012).
[44] DHS/ALL-004 General Information Technology Access Account Records, 77 FR 70792 (November 27, 2012).

- PIA: OpSTAR collects information from CBP employees and contractors but does not store any information from members of the public, therefore it has no PIA.
- Associated SORN(s): DHS/ALL-004 General Information Technology Access Account Records System of Records System (GITAARS)[45]

10. Human Resources Business Engine (HRBE)

The Human Resources Business Engine (HRBE) provides case management and Human Resource business process capabilities to CBP and its DHS component customers.

- PIA: DHS/CBP/PIA-032 Human Resources Business Engine[46]
- Associated SORN(s):
  - OPM/GOVT-1 General Personnel Records
  - OPM/GOVT-2 Employee Performance File System Records
  - OPM/GOVT-3 Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers
  - OPM/GOVT-5 Recruiting, Examining, and Placement Records
  - OPM/GOVT-6 Personnel Research and Test Validation Records
  - OPM/GOVT-7 Applicant Race, Sex, National Origin and Disability Status Records
  - OPM/GOVT-9 File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals, Fair Labor Standard Act (FLSA) Claims and Complaints, Federal Civilian Employee Compensation and Leave Claims, and Settlement of Accounts for Deceased Civilian Officers and Employees File on Position Classification Appeals, Job Grading Appeals, and Retained Grade or Pay Appeals, and Fair Labor Standard Act (FLSA) Claims and Complaints
  - OPM/GOVT-10 Employee Medical File System Records
  - DHS/ALL-018 Department of Homeland Security Grievances, Appeals, and Disciplinary Action Records System of Records
  - EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeal Records
  - DOL/GOVT-1 Office of Worker's Compensation Programs, Federal Employees' Compensation Act File

[45] DHS/ALL-004 General Information Technology Access Account Records, 77 FR 70792 (November 27, 2012).
[46] DHS/CBP/PIA-032 Human Resources Business Engine, *available at* www.dhs.gov/privacy.

- OGE/GOVT-1 Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program
- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS)
- DHS/ALL-016 Department of Homeland Security Correspondence Records
- DHS/ALL-021 Department of Homeland Security Contractors and Consultants
- DHS/ALL-022 Department of Homeland Security Drug Free Workplace

B. USCIS Sources/Systems

1. 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'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 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); CBP TECS (not an acronym). External systems include: 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[47]
- Associated SORN(s): Please see the PIA Appendix on page 18 of DHS/USCIS/PIA-010

2. 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 or in Mexico if they are deemed amenable to Migrant Protection Protocols (MPP), as outlined under Section 208 of the Immigration and Nationality Act (INA) (8 U.S.C. § 1158) and 8 CFR Part 208. 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[48]
- Associated SORN(s):
  - DHS/USCIS-001 Alien File, Index, and National File Tracking System of Records[49]
  - DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records[50]

[47] DHS/USCIS/PIA-010 Person Centric Query Service (April 2018), *available at* www.dhs.gov/privacy.

[48] DHS/USCIS/PIA-027 USCIS Asylum Division (September 2018), *available at* www.dhs.gov/privacy.

[49] DHS/USCIS-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (November 22, 2013).

[50] DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, 83 FR 36950 (July 31, 2018).

- DHS/USCIS-010 Asylum Information and Pre-Screening System of Records[51]

C. Non-DHS System/Sources

1. Department of Health and Human Services (HHS) Unaccompanied Alien Children (UAC) Portal

The Unaccompanied Alien Children (UAC) Portal was developed by HHS to manage information regarding the placement and care of UAC's apprehended by CBP. The UAC 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 UAC. The UAC portal collects and stores information related to UAC and their sponsors in the United States, who may be U.S. citizens.

Historically, HHS has provided CBP with a daily spreadsheet with the following types of information extracted from the UAC portal. The information listed below is not exhaustive; other data may be collected that is consistent with the general categories listed below.

- Personally Identifiable Information:
  - Name;
  - Aliases;
  - Date of birth;
  - Social Security number;
  - Alien Number;
  - Photographic identifiers;
  - Biometric identifiers;
  - Mother's maiden name;
  - E-mail address;
  - Mailing address;
  - Phone numbers;
  - Medical notes;
  - Financial accounts info;

[51] DHS/USCIS-0010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (November 30, 2015).

- Legal documents;
- Education records;
- Employment status, and;
- Passport number
- Family Status

In addition to biographical data and contact information for UAC and their sponsors, data related to the enforcement incident as well as placement process and requirements are captured:

- Case review details to include sponsor;
- Incidents;
- Medical screening;
- Education, and;
- Travel request information

CBP will use CBP EA to create visual representations of an individual's progression through various Federal agencies as part of the immigration enforcement process, including the location and duration of custody by HHS.

- PIA: HHS PIA for the Unaccompanied Alien Children Portal[52]
- Applicable SORN: 09-80-0321 ORR Division of Children's Services Records[53]

[52] *See* HHS PIA Unaccompanied Alien Children Portal, PIA Unique Identifier: P-9614390-049466, *available at* https://www.hhs.gov/sites/default/files/acf-uacp.pdf.

[53] 09-80-0321 ORR Division of Children's Services Records, 81 FR 46683 (November 18, 2016), 83 FR 6591 (February 14, 2018).