Privacy Impact Assessment
for the

Enterprise Management Information System-Enterprise Data Warehouse (EMIS-EDW)

DHS/CBP/PIA-034

September 7, 2016

Contact Point

Stephen P. Parshley
Office of Information and Technology
U.S. Customs and Border Protection
(571) 468-2674

Reviewing Official

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), operates the Enterprise Management Information System-Enterprise Data Warehouse (EMIS-EDW) to consolidate and present statistical information using reports and graphs using dashboard technology. EMIS-EDW warehouses current and historical data from various DHS source systems to provide timely statistical reports and trend analyses to management for situational awareness and the making of critical organizational decisions. CBP is conducting this PIA to assess the privacy risks of this information technology system and to notify the public of the collection, storage, retention, use, and dissemination of information belonging to members of the public that resides within EMIS-EDW.

Overview

EMIS-EDW extracts and consolidates information from multiple sources to present management with timely statistics and trend analysis for situational awareness and the making of critical organizational decisions. EMIS-EDW provides this information to CBP managers and analysts through dashboard technology using historical data from various DHS source systems. For example, EMIS-EDW provides users with access to automated statistical measures such as: number(s) of seizures, anti-terrorism matches, cargo processing rates, passenger processing rates, and enforcement actions from multiple data sources (please see Appendix A for a full list of reports and metrics generated by EMIS-EDW).

The EMIS portion of the system interfaces with the source systems, retrieves the information, and then stores the extracted information in the EDW portion of the system. Then, EMIS pulls data from EDW and associated data-marts[1] for cross-functional reports and analytical processing. EMIS-EDW is used by a large number of CBP offices, including: Office of Field Operations (OFO), U.S. Border Patrol (USBP), Air and Marine Operations (AMO), Office of Intelligence (OI), National Targeting Center (NTC), and Office of International Trade (OT), as well as other DHS components, namely U.S. Immigration and Customs Enforcement (ICE) and the Transportation Security Administration (TSA).

With one exception, EMIS-EDW refreshes information from the source systems every day, ranging from every 15 minutes to once a day depending on the purpose of the system. Extractions from the CBP Overtime Scheduling System (COSS) are refreshed once a week to coincide with the data update schedule of COSS. Ad-hoc requests also are available to a limited number of users to meet immediate business needs that are not addressed in standard dashboards and existing reports. Data is provided at the national, field office, and port of entry levels, as well as at the

[1] A customized subset of data in the warehouse designed to meet the specific business needs of a particular user or office.

operational or grand total level. EMIS-EDW expedites the aggregation of data, which: 1) reduces the administrative burden on users by consolidating information from many source systems; 2) displays the data in a user-friendly way; and 3) reduces the volume of demands placed on source systems for reporting information.

EMIS-EDW reports may include the following types of personally identifiable information (PII): general biographic information, citizenship and immigration information, criminal history, contact information, criminal associations, family relationships, level of education, and import-export history. The tools within EMIS-EDW are used to analyze and visualize aggregated statistic and trend data. Although EMIS-EDW uses data at the individual level to complie reports, all reports and analysis are presented at the aggregate level. EMIS-EDW is not designed to search existing information for enforcement and investigation purposes.

EMIS-EDW is comprised of the following standard reporting and analysis dashboards:

- Manager's Dashboard (MD) – provides information about intelligence (summaries and details of investigative records created for various program categories, known as "Memorandum of Information Records (MOIR)"), leave data, and overtime data for CBP Officers.
- BorderStat (BST) Dashboard – allows CBP management to monitor and analyze operational metrics so that trends, both positive and negative, can be quickly brought to the attention of senior CBP leadership. Data is displayed in high-level graphs, from which end users can drill down to specific transactions. BST provides data about seizures, primary passenger processing, passenger and vehicle primary queries, passenger and vehicle secondary processing, apprehensions and enforcement, I-94 passenger arrival/departures,[2] etc., as specified in Section 2.1.
- Airport Wait Time (AWT) Dashboard – captures data related to the "wait times" or delays experienced by individuals or cargo and conveyances arriving at the Points of Entry (POE) for admission or entry to the United States. It provides aggregated operational measures for cargo (approximate measures) and passenger processing at ports of entry.
- Western Hemisphere Travel Initiative (WHTI)[3] Dashboard – provides a dashboard to view key WHTI metrics including U.S./Canadian citizenship compliance, query rate, radio frequency identification (RFID)[4] document read rate, etc. WHTI collects data for certain passengers arriving from foreign travel points to the United States.

[2] DHS/CBP/PIA-016 U.S. Customs and Border Protection Form I-94 Automation (February 27, 2013), *available at*: https://www.dhs.gov/publication/us-customs-and-border-protection-form-i-94-automation.
[3] DHS/CBP/PIA-004 Western Hemisphere Travel Initiative (August 11, 2006), as well as subsequent updates, *available at:* https://www.dhs.gov/publication/beyond-border-entryexit-program-phase-ii.
[4] Radio-frequency identification (RFID) technology uses electromagnetic fields to automatically identify

- Targeting and Analysis Systems Program Directorate (TASPD) Security Dashboard – provides an informational reporting dashboard for use by TASPD Security Team/Information System Security Officers (ISSO) to review audit logs for operational systems.
- Workload Staffing Model (WSM) Dashboard – is a decision support tool for the allocation, estimation, and assignment of staffing.
- Cargo Enforcement Reporting and Tracking System (CERTS) Dashboard – provides a dashboard to view various reports and analytics corresponding to the examinations performed on all inbound shipments (limited by data entry accuracy, completeness, and consistency).
- Centers of Excellence and Expertise (CEE) Dashboard – provides aggregated operation measures for cargo processed by the CEEs, including validation, facilitation, and enforcement.

EMIS-EDW extracts information from multiple source systems to create reports and perform analyses. More specifically, EMIS-EDW:

- Consolidates the key reporting measures from multiple source systems into one single data repository.
- Provides a measurement environment for all air, land, and sea ports of entry for passenger travel (listed in Appendix B).
- Provides CBP headquarters (HQ) with statistics for research purposes.
- Provides District Field Officers and Port Directors with statistical information for their respective field offices and ports of entry, enabling trend analysis of data elements without having to depend upon their local data.

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?

EMIS-EDW is authorized to collect and maintain records pursuant to the following authorities granted to the source systems:

- 8 U.S.C § 1357;
- 19 U.S.C. §§ 482, 1461, 1496, 1581, 1582;
- 49 U.S.C. § 44909;
- Enhanced Border Security and Visa Reform Act of 2002 (Pub. L. 107-173);

and track tags attached to objects. The tags contain electronically stored information.

- Trade Act of 2002 (Pub.L. 107-210);
- Intelligence Reform and Terrorism Prevention Act of 2004 (Pub.L. 108-458); and
- Security and Accountability for Every Port Act of 2006 (Pub. L. 109-347).

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

EMIS-EDW extracts data from several source systems covered under multiple SORNs. These SORNs are listed in Appendix C.

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

Yes, a Security Plan for EMIS-EDW was completed and an Authority to Operate was granted to EMIS-EDW to on September 11, 2014.

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

CBP Records Office is currently drafting a Record Retention Schedule for EMIS-EDW for data specific to EMIS-EDW, i.e. reports and analyses. CBP has proposed to retain data specific to EMIS-EDW for for seven years and then archived for up to 40 years. Cost and performance impact of data retention may lead to retention periods less than 40 years.

To the extent information is ingested from other systems, data is retained in EMIS-EDW in accordance with the record retention requirements of those systems.

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.

PRA does not apply to EMIS-EDW because EMIS-EDW does not collect information directly from members of the public. The PRA applies to many of the underlying data collectios that do collect directly from the public.

Section 2.0 Characterization of the Information

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

The data collected by EMIS-EDW can be generally described as:

- Information about importers, brokers, carriers, shippers, buyers, sellers, and crew who facilitate the importation of cargo into the United States. This information includes: name, address, birth date, and government-issued identifying records, when available and applicable.
- Information about exporters, brokers, carriers, shippers, buyers, sellers, and crew who facilitate the exportation of cargo from the United States. This information includes: name, address, birth date, government-issued identifying records, when available and applicable.
- Information about passengers and crew entering or departing (and in some cases overflying) the United States. This data includes passenger and crew manifests (through the Advance Passenger Information System (APIS)[5], information collected during secondary inspections, and seizure records. This data may include such items as name, address, and flight.
- Information about vehicles and persons entering the United States at land border ports of entry. This data may include license plate numbers for vehicles entering the United States.
- Information about seizures, apprehensions, inadmissibility decisions, and other enforcement actions related to secondary processing activities (activities are not linked in the data). This information includes: name, address, birth date, and government-issued identifying records, when available and applicable.
- Annual leave, sick leave, and overtime data for CBP officers. This information includes: CBP officer's name and location, when available and applicable.
- Aggregated measures of the data stated above to enable statistical reporting and analysis of trends.

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

EMIS-EDW receives various data at a regularly scheduled intervals of time (i.e., hourly, daily, or weekly) from multiple source systems. There are automated Extract-Transform-Load

[5] DHS/CBP/PIA-001(f) Advance Passenger Information System (APIS) (June 5, 2013), *available at:* https://www.dhs.gov/sites/default/files/publications/privacy-pia-apis-update-20130605_0.pdf.

(ETL) processes that allow data to be captured from these sources at regularly scheduled intervals, and loads them into the data warehouse for reporting functions. EMIS-EDW extracts data from the following source systems:

- ATS[6] – a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based targeting scenarios and assessments.
    - ATS-N – Automated Targeting System-Inbound is the source system for cargo data and associated reference data.
    - ATS-CERT – is the source system for cargo exam findings data and associated reference data.
    - ATS-P – Automated Targeting System-Passenger is the source for primary processing, secondary processing, Advanced Passenger Information System (APIS), I-94 visa information, and seizure data.
- CBP Overtime Scheduling System (COSS)[7] – is the source for employee leave balance and overtime data.
- Automated Commercial Environment (ACE)[8] – is the source for CBP CEE importers and trade partner accounts.
- Automated Commercial System (ACS)[9] – is the source for information to track, control, and process all goods imported into the United States.
- Enforcement Case Tracking System E3/ENFORCE[10] – is the source for USBP assault, seizure, inadmissibility, apprehension, manpower, and program data.
- Student and Exchange Visitor Information System (SEVIS)[11] – is the source for Student

[6] DHS/CBP/PIA-006 Automated Targeting System (ATS), and subsequent updates, *available at:* https://www.dhs.gov/publication/automated-targeting-system-ats-update.

[7] DHS/ALL/PIA-053 DHS Financial Management Systems (July 30, 2015), *available at:* https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhswide-financialmgmtsystem-july2015.pdf.

[8] DHS/CBP/PIA-003(b) Automated Commercial Environment (ACE) (July 31, 2015), *available at:* https://www.dhs.gov/publication/filing-data-acsace.

[9] Now part of ACE and covered by the ACE PIA.

[10] DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT (July 25, 2012), *available at:* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-e3.pdf.

[11] DHS/ICE/PIA-001(a) Student Exchange Visitor Information System (SEVIS) (June 23, 2011), *available at:* https://www.dhs.gov/publication/dhsicepia-%E2%80%93-001a-student-exchange-visitor-information-system-sevis.

Exchange Visitor Program data.

- Enforcement Support Systems (ESS)[12] – is the source for Significant Incident Report incidents and scheduling data.
- Seized Currency and Asset Tracking System (SEACATS)[13] – is the source for case management and seizure data for the Office of Investigation and OFO respectively. It includes seized assets information, biographical and identifying data, and subject arrest information necessary to conduct asset forfeiture proceedings.
- Firearms, Armor, and Credentials Tracking System (FACTS)[14] – is the source for CBP and ICE Firearms and Badge/Credentials data.
- Tasking, Operations, and Management Information System (TOMIS)[15] – is the source for AMO missions, segments, and other measures.
- REMEDY[16] – is the source for USBP Remote Video Surveillance System equipment operational status. It includes asset name, identification information, type, equipment quantities, and its current operational or non-operational status.
- Performance and Learning Management System (PALMS)[17] – is the DHS source for employee training courses and curriculum data.
- TECS[18] – is the source for data required for CBP Office of Professional Responsibility (OPR), Homeland Security Investigations, and OPR investigation activities.
- Intelligent Computer Assisted Detection (ICAD)[19] – is the source for USBP sensor data. Underground sensors installed along the U.S. border detect various types of activity and

[12] ESS will be covered by the forthcoming PIA.
[13] SEACATS will be covered by the forthcoming PIA.
[14] FACTS is covered under DHS/ALL-010 DHS Security Asset Management Records System of Records (October 23, 2008), 73 FR 63181, *available at: https://www.gpo.gov/fdsys/pkg/FR-2008-10-23/html/E8-25207.htm*.
[15] DHS/ALL-004 – General Information Technology Access Account Records System (GITAARS) (November 27, 2012), 77 FR 70792, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm.
[16] DHS/CBP/PIA-029 REMEDY Enterprise Services Management System (April 28, 2016), *available at:* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-remedy-april2016.pdf.
[17] DHS/ALL/PIA-049 Performance and Learning Management System (PALMS) (January 23, 2015*),* *available at:* https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-palms-01232015.pdf.
[18] DHS/CBP/PIA-009(a) TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative (August 5, 2011), *available at:* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-tecs-sar-update_0.pdf.
[19] DHS/CBP/PIA-022 Border Surveillance Systems (BSS) (August 29, 2014), *available at:* https://www.dhs.gov/sites/default/files/publications/privacy_pia_CBP_BSS_August2014.pdf.

relay that information to the receiver/decoder located at the sector headquarters. This data includes identification number, type, alarm level, timers, paths, ticket type, and GPS location. This is a source for reports on ticket, dispatch, and sensor data.

- National Distribution Center (NDC) Mainframe – is the source for CBP employee identification data by organization and office from Web-Tele (web and telephone emergency contact information).

Data is available at the national, field office, and individual port levels, and is displayed as summary, aggregate, and transaction-level data in reports that are refreshed daily.

EMIS-EDW is exclusively a reporting system, and it does not collect additional information directly from individuals. All PII comes from the source systems. This information is collected by CBP source systems to assist in the CBP law enforcement mission related to the import or export of cargo and the entry or exit of persons from the United States; internal investigations; and administrative personnel activities.

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, EMIS-EDW does not use any commercial or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

EMIS-EDW relies upon the source systems to ensure that data used by EMIS-EDW is accurate and complete. Discrepancies may be identified in the context of a CBP officer's review of the data, and when discovered, the CBP officer will take action to correct that information in the source system. EMIS-EDW monitors source systems for changes to the source system databases. All of the updates that occur in the source systems, along with new data entered in the source systems, are loaded into EMIS-EDW using ETL processes at regularly scheduled intervals.

When corrections are made to data in source systems, the updated information is uploaded into EMIS-EDW at the established intervals, ensuring that only the most current data is used for reporting within EMIS-EDW. In this way, EMIS-EDW integrates the most current data from the source systems.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Information in EMIS-EDW may not be as timely as the source systems.

Mitigation: With the exception of COSS, EMIS-EDW information is collected from the source systems and updated one or more times a day. Data is modified in or added to EDW when it is modified in or added to a source system. COSS information is refreshed on a weekly basis when the source system is updated.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

EMIS-EDW serves solely as a data reporting system and therefore, does not update operational data. Automated operations move data from the source systems and make it available for reports and analyses. Authorized CBP officers and other Government personnel located at the Washington, D.C. headquarters, field offices, sectors, port of entries, and stations use EMIS-EDW to support their statistical reporting and historical data analysis related requirements.

EMIS-EDW enables CBP management to look at trends and historical data that are critical to detailing CBP work and effectiveness. The automated nature of EMIS-EDW increases the efficiency and effectiveness of CBP managers at all levels within the CBP organization to identify new trends and provide statistical analysis. The EMIS-EDW displays selected metrics, comparisons, and reports to provide port of entry/field personnel with tangible measures of performance and operation. High-level graphs and reports also enable users to access the underlying transactions, so that a comprehensive understanding of the data can be achieved. Various data visualization web controls, such as speedometers and interactive metric trends, provide graphic and easily understood performance measures. Business analysts also have the ability to create their own custom reports/queries and save them for future use. The use of EMIS-EDW eliminates preivously manual, time-intesive processes.

Authorized users have access to the EMIS-EDW dashboards for purposes of statistical reporting. CBP may grant access to EMIS-EDW to other DHS components or offices that have a need for the aggregated report information in the performance of their duties under 5 U.S.C. §552a(b)(1) consistent with U.S. law, DHS and CBP policy, and any applicable arrangements or agreements. These purposes may include DHS mission-related functions, as well as associated testing, training, management reporting, planning, and analysis. Providing other DHS components or offices with access to EMIS-EDW does not allow them to access the underlying source system data.

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.

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

Yes. In addition to the CBP users, EMIS-EDW is also used by DHS components, namely ICE and TSA. In addition, aggregated reporting information from EMIS-EDW may be shared with components within DHS on a need to know basis consistent with the component's mission pursuant to section 552a(b)(1) of the Privacy Act. Access to EMIS-EDW is role-based and assigned according to the mission of the component and the user's need to know. Access to specific reports and dashboards within EMIS-EDW is further controlled by providing each user with access to only those functions required to perform his or her duties.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: The information may be used for purposes inconsistent with the purpose for which it was collected.

Mitigation: This risk is mitigated through the extensive training that is provided to CBP officers in the appropriate use of the collected information. As a statistical reporting system, EMIS-EDW does not allow for the search of specific individuals, nor is it possible to conduct a search using PII. The information is used by CBP management to create daily, weekly, monthly, and yearly reports containing key performance measures reflecting CBP operations. These reports do not contain any PII. It is not intended to be used by CBP officers in identifying individuals or cargo that may pose a risk of violating U.S. laws or that otherwise represent a threat to national security, and it does not replace the officer's discretion to validate the aggregated data being presented to them.

Privacy Risk: EMIS-EDW stores copies of many operational data sets, and may be accessed by unauthorized users.

Mitigation: EMIS-EDW employs both system level security and application level security, including role-based access control and discretionary access controls. EMIS-EDW has also undergone the Security Authorization process, during which all security documentation (i.e., Security Plan, Contingency Plan, Risk Assessments and Security Assessments, Interconnection Security Agreements) were updated prior to the issuance of the system's Authority to Operate (ATO) date. CBP conducts routine audits and system checks to ensure the relevance of controls and markings, and to protect the information over time.

EMIS-EDW's role-based access is highly restricted and audited. Access is restricted in the form of Mandatory Access Control, which is based on a demonstrated "need to know." Data may only be accessed through the CBP network (via the DHS intranet) using encrypted passwords and user sign-on. All individuals with access to EMIS-EDW are required to complete security and data privacy training on an annual basis and their usage of the system is audited to ensure compliance with all privacy and data security requirements.

EMIS-EDW is hosted at the National Data Center (NDC). NDC is a secure, access-controlled facility with physical security and protective services 24 hours per day, 7 days per week. The computer room is further restricted to a controlled list of authorized individuals. The building floors are occupied by CBP personnel who are required to pass a security background investigation. No non-Government system hosting is involved.

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.

EMIS-EDW does not collect any information directly from individuals. All of the information that is used for reporting in EMIS-EDW is extracted from other CBP Government data sources identified in Section 2.2. Depending on the source system, notice may have been provided by Privacy Act Statements or applicable source system SORNs (see Appendix C) and PIAs.

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 EMIS-EDW because EMIS-EDW is not the source system. Depending on the source system, individuals may have had the opportunity to consent, decline, or opt out at the time the information was collected.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: The individual may not be aware that the information is being used by EMIS-EDW.

Mitigation: This risk is only partially mitigated. Although individuals may receive notice through the source systems' PIAs and SORNs, they may not be aware that their information has been copied to EMIS-EDW. This risk is partially mitigated through the publication of this EMIS-EDW PIA. In addition, any reports or analyses created within EMIS-EDW are presented in aggregate, and therefore, individual information is not available to system users.

Section 5.0 Data Retention by the Project

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

The retention period for data in EMIS-EDW reflects the underlying retention period for the data in its source systems. For example, since the data from ATS is retained for six years, the associated information in EMIS-EDW is retained for the same period of time.

EMIS-EDW staff are working with the CBP Records Office on a proposed NARA retention schedule for the EMIS-EDW reports and analyses. The proposed retention schedule is as follows: data will be retained for seven years after which time it will be archived for up to 40 years. Cost and performance impact of data retention may lead to retention periods less than 40 years.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: EMIS-EDW may retain data longer than the source systems' retention periods.

Mitigation: This risk is partially mitigated. EMIS-EDW has implemented controls that coordinate the automatic deletion of the data with the source system's retention schedule. With one exception, EMIS-EDW refreshes information from the source systems every day, ranging from every 15 minutes to once a day depending on the purpose of the system.[20] Upon refresh from the source systems, data is deleted from EMIS-EDW when it is removed from a source system. This type of deletion makes the data inaccessible to regular users. However, this risk is only partially mitigated because EMIS-EDW still retains deleted information in an archive. This historical data will be retained in accordance with the proposed EMIS-EDW record retention schedule.

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.

No, the information in the EMIS-EDW system is not shared outside of DHS as part of the normal agency operations.

[20] Extractions from the CBP Overtime Scheduling System (COSS) are refreshed once a week to coincide with the data update schedule of COSS.

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

EMIS-EDW does not share information outside of DHS.

6.3 Does the project place limitations on re-dissemination?

EMIS-EDW does not support users outside of DHS. Data maintained in EMIS-EDW may be shared with any DHS components or offices that have a need for the information in the performance of their duties.

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

EMIS-EDW uses the existing processes and procedures within DHS and CBP for recording disclosures of information as appropriate to the situation, and does not establish or maintain an additional record of the disclosures within the EMIS-EDW system. Approved internal forms are used to keep a record of disclosures.

6.5 Privacy Impact Analysis: Related to Information Sharing

There is no risk to information sharing because PII is not shared outside of DHS from EMIS-EDW.

Section 7.0 Redress

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

Information within EMIS-EDW originates with the source system. As a result, individuals can gain access to their information by following the access procedures outlined in the PIAs and SORNs of the source systems.

In addition, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a Freedom of Information Act (FOIA) or Privacy Act request in writing to:

U.S. Customs and Border Protection
FOIA Division
90 K Street, NE, 9th Floor
Washington, D.C. 20229

FOIA 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.

Specific FOIA contact information can be found at http://www.dhs.gov/foia under *Contact Information*.

Requests should conform to the requirements of 6 CFR Part 5, which provides the rules for requesting access to Privacy Act records maintained by DHS. The envelope and letter should be clearly marked "Privacy Act Access Request". An individual must first verify his/her identity, meaning that he/she must provide full name, current address, and date and place of birth. The request must include a notarized signature or be submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, forms for this purpose may be obtained from the Director, Disclosure and FOIA, http://www.dhs.gov/foia or 1–866–431–0486. In addition, the following should be provided:

- An explanation of why the individual believes DHS would have information on him/her;
- details outlining when he/she believes the records would have been created;
- and if the request is seeking records pertaining to another living individual, it must include a statement from that individual certifying his/her agreement for access to his/her records.

Without this bulleted information, CBP may not be able to conduct an effective search, and the request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CBP notes that EMIS-EDW is a statistical reporting tool that extracts data from various databases, but does not actively collect the information in those respective databases. When an individual is seeking redress for other information analyzed in EMIS-EDW, such redress is properly accomplished by referring to the databases that directly collect that information. If individuals are uncertain what agency handles the information, they may seek redress through the DHS Traveler Redress Program ("TRIP") (See 72 Fed. Reg. 2294, dated January 18, 2007), described below.

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

EMIS-EDW extracts data from other CBP/DHS systems identified in Section 2.2. Procedures for correcting inaccurate or erroneous information will be handled by these source systems as appropriate. EMIS-EDW incorporates the procedures of the source systems with respect to error correction. Once any updates or corrections are made in the source systems, they are transmitted to EMIS-EDW. Corrected data becomes available to EMIS-EDW via regularly scheduled ETL processes. These ETL processes detect the updated records in the source systems and appropriately update the same records in EMIS-EDW. EMIS-EDW monitors source systems for changes to the source system databases. When corrections are made to data in source systems, EMIS-EDW reflects these updates to data, accordingly.

Individuals may seek redress and/or contest a record through two different means. Both will be handled in the same fashion. If the individual is aware the information is specifically handled by CBP, requests may be sent directly to CBP FOIA (via the procedures described above) If the individual is uncertain what agency is responsible for maintaining the information, redress requests may be sent to DHS TRIP at DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA- 901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip.

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

Upon request, CBP officers may provide a fact sheet that provides information on appropriate redress. The redress procedure provides the ability to correct data in the source systems. Additional information is available on DHS's website. The source system SORNs also provide information on accessing and amending information collected through those systems.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Because EMIS-EDW maintains copies of information from source systems, records corrected as part of the redress, correction, or amendment process may not be updated immediately in EMIS-EDW.

Mitigation: This risk is mitigated by the frequency in which information is updated or refreshed in EMIS-EDW. EMIS-EDW is updated or refreshed when the information in the source system is updated. With the exception of one source system, these updates occur every day, ranging from every 15 minutes to once a day. As a result, when a record is modified or corrected in the source system, it also is modified or corrected in EMIS-EDW. Therefore, if individuals follow the procedures outlined in section 7.2 for correction of their information in the source system, redress also will be realized in EMIS-EDW. Source systems are identified at the bottom of each report generated by EMIS-EDW.

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?

EMIS-EDW has role-based access, which limits the system access of users as defined by each specific user's profile and his/her prescribed rights and responsibilities of each user. Access by users, managers, system administrators, developers, and others to EMIS-EDW data is defined in the same manner and employs profiles to tailor access to the user's mission or operational functions. EMIS-EDW user roles are highly restricted and audited. User roles are based on a demonstrated need to know related to the performance of an individual's job-related duties. Data may only be accessed using the CBP network (via the DHS intranet), which requires encrypted passwords and user sign-on. All EMIS-EDW users are required to complete security and data privacy training on an annual basis, and their usage of the system is audited to ensure compliance with all privacy and data security requirements.

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

CBP process owners and all system users are required to complete annual security training such as the "CBP Sensitive Security Information," "CBP IT Security Incident Response Training," "CBP Safeguarding Classified National Security Information," and "CBP IT Security Awareness and Rules of Behavior Training" through PALMS. Each PALMS security training addresses the appropriate use of PII. If an individual does not take training, that individual will lose access to all computer systems. All EMIS-EDW users must also completed the annual DHS privacy awareness training.

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

EMIS-EDW uses ATS Entitlement for end-user authentication. Initial requests for grants to the system are routed from the user through his/her supervisor to the specific CBP Process Owners. Need-to-know determinations are made at both the supervisor and process owner level. If validated, the request is passed on to the Security Help Desk. Once received, System Security Personnel determine the user Background Investigation (BI) status.

Once the BI is validated, the user's new profile changes are implemented. The user, supervisor, and Process Owner are notified via email that the request has been processed along with instructions for the initial login. User request records with any additional information provided by approving authorities are maintained by CBP. Profile modification requests follow the same process as for an initial request. If an individual has not used the system for more than 90 days, that individual's access will be denied and the same procedures noted above must be completed to renew access. Access is reviewed by the process owner periodically to ensure that only appropriate individuals have access to the system.

Each user group's[21] access to the system is defined by the specific profile created for that group. Group profiles are intended to limit access by reference to the common rights and mission

[21] Profile set in the system for different access levels.

responsibilities of users within the group. Access by Users, Managers, System Administrators, Developers, and others to the EMIS-EDW data is defined in the same manner and employs profiles to tailor access to mission or operational functions. User access to data is based on a demonstrated need-to-know by a user.

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

Memoranda of Understanding (MOUs) are created by the business owners with input from the program managers. The MOUs are internal only within DHS. Any new uses of the information and new access to the system are reviewed and approved by updating the MOUs. MOUs for EMIS-EDW are sent to the CBP Privacy Officer for review and to DHS for final approval.

Responsible Officials

Stephen P. Parshley
Advanced Analytics Branch
Department of Homeland Security
Office of Information Technology
U.S. Customs and Border Protection

Debra L. Danisek
Acting Privacy Officer
Office of Privacy and Diversity
Office of the Commissioner
U.S. Customs and Border Protection

Approval Signature

Original signed copy on file with the DHS Privacy Office.

____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Appendix A:

Enterprise Management Information System – Enterprise Data Warehouse (EMIS-EDW) Metrics

The EMIS-EDW metrics is a standard of measure of a degree to which a dashboard possesses some property. Metrics are available via standard reporting and analysis dashboards. A dashboard is an easy to read, often single page, real-time user interface, showing a graphical presentation of the current status (snapshot) and historical trends of an organization's or computer appliances key performance indicators to enable instantaneous and informed decisions to be made at a glance.

Access to the EMIS-EDW is subject to the eligibility requirements (i.e., clearance level or demonstrated and approved business/operational need). EMIS-EDW access is based on approved CBP system security requirements, and is consistent with Targeting and Analysis Program Directorate (TASPD) Policy and Procedures, Office of Information Technology (OIT) Policies, and CBP 1400-05D Policy and Procedures Handbook.

The following list identifies the metrics by dashboard. Descriptions of the dashboards are provided below.

BorderStat Dashboard

- Total Drug Seizures by Weight
- Total Drug Seizures by Line Item Count
- Total Drug Seizures by Incident Count
- Total Currency Seizures by Amount (USD)
- Total Currency Seizures by Line Item Count
- Total Currency Reporting Violation Amount (USD)
- Total Currency Reporting Violation Line Item Count
- Total Merchandise Seizures by Line Item Count
- Total Arrests
- Total Weapons Seizures Line Item Count
- Unapproved Seizures Under 24Hrs
- Unapproved Seizures Between 24Hrs and 72Hrs

- Unapproved Seizures Over 72Hrs
- Total Primary Vehicle Queries
- Total Primary Name Queries
- Total IO25 Secondary Inspection Results
- Total IO95 Secondary Inspection Results
- Total IO04 Secondary Inspection Results
- Total Inadmissible broken down by Field Office / Ports
- Total National Security Intercepts
- *Top 10:* Top 10 Dispositions, Top 10 Nationalities, and Top 10 Deferred Inspections
- Total Inadmissible
- Total Inadmissible Turned Away
- Total Inadmissible Not Turned Away
- Total Enforcement Actions
- Total Apprehensions
- Total Mexican Apprehensions
- Total Office of Transportation Management Apprehensions
- Total Australian Securities and Investments Commission Apprehensions
- Total Inadmissible Comparison
- Total Inadmissible by Points of Entry (POE)
- Total Inadmissible by Nationality
- National Inadmissible Snapshot
- Enforcement Actions Comparison
- Fraudulent Documents Comparison
- Enforcement Actions by POE
- Enforcement Actions by Nationality
- National Enforcement Actions Snapshot
- Stowaways, Absconders, and Deserters Comparison

- Total Inadmissible Count
- Inadmissible Turned Away Count
- Inadmissible Not Turned Away Count
- Total Enforcement Actions
- Total Aliens Smuggled
- Total Criminal Alien Encountered
- Total False Claims
- Total Fraud Docs
- Total National Security Intercepts
- Total Smugglers
- Total Stowaways Absconders Deserters Count
- All Other Dispositions Count
- Positive Terrorist Identities Datamart Environment (TIDE) Matches Count
- Suspected Positive TIDE Match Count
- Flight and Vessel Transmissions Query Hits Count
- Flight and Vessel Transmissions Count
- Flight and Vessel Passenger Count
- I-94 Admission Count
- Total I-94 Issued Count
- Top 20 Importers (By Office of Field Operations (OFO) and by POEs)
- Top 20 Commodities (By OFO and by POEs)
- Top 20 Trading Partners (Country of Origin) (By Field Office and by POEs)
- Average Number of Shipments/Bill of Lading (BOL)/Entries per day
- Average Number of Shipments/BOL/Entries by mode other than Mail (MOT)
- Top 20 POEs by Volume by MOT
- Number of Shipments
- Number of Manifests

- Number of BOLs
- Number of Entries
- Number of Containers
- Cargo Release User-Defined Rules (UDR) Discrepancies Count
- Entry Summary UDR Discrepancies Count
- Cargo Release UDR Discrepancies Count

Airport Wait Time Dashboard

- Flights with Average Wait Time greater than 60 minutes
- Flights with More than 3% of passengers having wait time greater than 60 minutes
- Average Wait Time (mins)
- Max Wait Time
- Passenger Counts By Wait Time Intervals
- Average Wait Time by Admission Class in mins
- Terminal Wait Time
- Office of Attorney General Schedule by Hour

Western Hemisphere Travel Initiative (WHTI) Dashboard

- WHTI compliance rates for the U.S. and Canadian travelers
- Query rates and Radio-Frequency Identification Device (RFID) Saturation Rates and Document Usage Rates
- Border Wait times
- Peak Vehicle Wait Time
- Count of Fraudulent Docs by Date and POE
- WHTI Referrals for IO95 and IO04
- RFID Saturation Trends
- Estimated Query Rate Values

- Estimated Query Rate Trends

Workload Staffing Model Dashboard

- Estimated Workload Staffing count of cargo and passenger environments

Manager's Dashboard

- Regular Overtime Amount
- Premium Amount
- Cap Compliance
- Annual and Sick Leave trends
- Total Memoranda of Information Received (MOIR) Count
- MOIRs Current Year Status
- MOIRs Subject Record Status
- MOIRs Subject Record Type Count
- MOIRs Comparative Status
- MOIRs Count by Category Type

Targeting & Analysis Systems Program Directorate (TASPD) Security Dashboard

- Informational reporting tool
- Intended for TASPD security team/Information System Security Officers to review audit logs
- Intended to eventually provide audit log information for every TASPD system.

Cargo Enforcement Reporting and Tracking System (CERTS) Dashboard

- Provides the users with reports and analytics corresponding to the examinations performed on all inbound Cargo that is captured within the CERTS application.
- Ad hoc reports of data on shipments, bill, and entries.

- Reports that provide summary and detailed information on all inbound High Risk Shipments that arrived into the United States.
- One-click reports on Tools and Methods Usage, Exam Findings, and Homeland Security Seals.

Centers of Excellence and Expertise (CEE) Dashboard

- Provide capability for Validation, Facilitation, and Enforcement of CEE trade policies.
- Weekly reports of validation section.
- UDRs fired on Cargo Release and Entry Summaries filed by CEE Importers.

Appendix B: EMIS-EDW Metrics By Subject Area

The metrics, available in EMIS-EDW, are organized by subject area. The EMIS-EDW provides metrics across multiple subject areas. The following list identifies how the data can be accessed:

- Seizures – Seizure, Narcotics, Currency, and Property Seizures reports
- Primary and Secondary processing – Passenger, Vehicle, and Cargo reports
- Enforcement – Apprehension, Inadmissible, and Enforcement Action reports
- Anti-terrorism – Terrorist Screening Database reports
- Bill, Entry, and Entry Summary processing reports
- S2 High Risk Cargo reports for all modes of transportation
- Budget and Overtime Expenditure – CBP Personnel Scorecard and Cap Compliance reports
- Intel – Memorandum of Investigative reports
- Airport Wait Time reports and Flight log
- WHTI dashboard and reports
- Container Security Initiative reports
- NTC-C Workload reports
- NTC-P Hotlist and other reports
- Centers of Excellence and Expertise (Dashboards: Weekly Report, Importer Profile, Facilitation Dashboards, Validations Dashboards, Enforcement Profile, D.C. HQ Dashboards (metrics of Office of Trade)
- Oracle Business Intelligence Enterprise Edition (OBIEE) User-Defined Rules (UDR) Performance Dashboard: Entry Summary UDR Performance, Cargo Release UDR Performance, Bill of Lading UDR Performance
- OBIEE Entry Summary Dashboard: entry summary trend analysis

Appendix C: SORNS Covering Systems From Which Data is Extracted by EMIS-EDW

- OPM/GOVT-1 General Personnel Records System of Records (December 11, 2012), 77 FR 73694, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2012-12-11/html/2012-29777.htm
- OPM/GOVT-2 Employee Performance File System of Records (June 19, 2006), 71 FR 35342, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2006-06-19/html/06-5459.htm
- GSA/GOVT-3 Travel Charge Card Program System of Records (April 3, 2013), 78 FR 20108, *available at:* http://www.gsa.gov/portal/mediaId/205395/fileName/2013-07669.action
- DHS/ALL-002 Department of Homeland Security Mailing and Other Lists System, System of Records (November 25, 2008), 73 FR 1659, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2008-11-25/html/E8-28053.htm
- DHS/ALL-003 Department of Homeland Security General Training Records System of Records (November 25, 2008), 73 FR 1656, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2008-11-25/html/E8-28037.htm
- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) (November 27, 2012), 77 FR 70792, *available at*: https://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm
- DHS/ALL-007 Department of Homeland Security Accounts Payable System of Records (September 28, 2015), 80 FR58286, *available at*: https://www.gpo.gov/fdsys/pkg/FR-2015-09-28/html/2015-24587.htm
- DHS/ALL-008 Department of Homeland Security Accounts Receivable System of Records (September 28, 2015), 80 FR 58289, *available at*: https://www.gpo.gov/fdsys/pkg/FR-2015-09-28/html/2015-24588.htm
- DHS/ALL-010 Department of Homeland Security Asset Management Records System of Records (September 28, 2015), 80 FR 58280, *available at*: https://www.gpo.gov/fdsys/pkg/FR-2015-09-28/html/2015-24583.htm
- DHS/ALL-019 Department of Homeland Security Payroll, Personnel, and Time and Attendance Records System of Records (September 28, 2015), 80 FR 58283, *available at*: https://www.gpo.gov/fdsys/pkg/FR-2015-09-28/html/2015-24589.htm

- DHS/ALL-037 E-Authentication Records System of Records (August 11, 2014), 79 FR 46857, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2014-08-11/html/2014-18703.htm
- DHS/CBP-002 Global Enrollment System, System of Records Notice (January 16, 2013), 78 FR 3441, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2013-01-16/html/2013-00804.htm
- DHS/CBP-005 Advance Passenger Information System (APIS) System of Records (March 13, 2015), 80 FR 13407, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2015-03-13/html/2015-05798.htm
- DHS/CBP-006 Automated Targeting System (ATS) System of Records (May 22, 2012), 77 FR 30297, *available at*: http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm
- DHS/CBP-011 U.S. Customs and Border Protection TECS System of Records (December 19, 2008), 73 FR 77778, *available at*: https://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm
- DHS/ICE-001 Student and Exchange Visitor Information System, System of Records (January 5, 2010), 75 FR 412, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2010-01-05/html/E9-31268.htm
- DHS/ICE-004 Bond Management Information System (BMIS) System of Records (August 19, 2009), 76 FR 8761, *available at*: https://www.gpo.gov/fdsys/pkg/FR-2011-02-15/html/2011-3448.htm
- DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE) System of Records (April 30, 2015), 80 FR 24269, *available at*: https://www.gpo.gov/fdsys/pkg/FR-2015-04-30/html/2015-09615.htm
- DHS/NPPD-004 Department of Homeland Security Automated Biometric Identification System (IDENT) System of Records (June 5, 2007), 72 FR 31080 *available at:* https://www.gpo.gov/fdsys/pkg/FR-2007-06-05/html/07-2781.htm

Appendix D:

Enterprise Management Information System – Enterprise Data Warehouse (EMIS-EDW) – Advanced Analytic Tools

CBP is deploying various business intelligence (BI) tools to perform advanced analysis on DHS and other federal agency data available to CBP. Like the EMIS-EDW Metrics discussed in Appendix A, CBP will utilize existing data sets and commercial off-the-shelf (COTS) products to aggregate and provide customizable dashboards and graphical data displays to assist CBP in making operational decisions. A description of each tool and the dashboard created is provided below.

1. Data Cube – Athena

Athena uses Date Cube, a 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 betwen 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 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)

Key features of Athena:

- Does not retain source system information beyond what is displayed during a user session
- 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)

- Presents information in an interactive timeline and geo-spatial views

1.1. DataCube Athena - CBP Migrant Crisis Action Team (MCAT) Use Case (*approved April 8, 2019*)

The MCAT uses Athena to aggregate data elements from existing enterprise databases to create a customizable dashboard. The current migrant crisis reporting methods rely on disparate data sources that are owned by multiple government stakeholders, including CBP, ICE, and Department of Health and Human Services (HHS). As a result, users must manually pre-process the data in order to perform collaborative analysis. Manual pre-processing of data elements from multiple data sources requires significant resources and is prone to errors which can be detrimental to data accuracy. Athena enables users to aggregate disparate data sources, link related data elements, and visualize those elements in one view, which significantly reduces the time and effort required for CBP's Migrant Crisis Action Team members and ICE Agents to fulfill this mission.

Athena retains the following information on users of Athena:

- Hash ID

In addition, Athena will use the following information contained in the original data source:

- Name;
- Aliases;
- Address;
- Date of birth;
- Age;
- Event number;
- A-File number;
- FIN number;
- Citizenship;
- Gender;
- Visa number;
- Passport number;
- Seizure information;
- Apprehension information;
- Inadmissibility decisions;
- Other law enforcement actions related to primary and secondary processing activities (Processing activities are not explicitly stated or linked in the data);
- Information regarding law enforcement actions (related to primary and secondary processing activities):
  - Date/Time of an action;
  - Action code; and
  - Location/facility code associated with an action.

The following information will come from HHS UAC data source. HHS UAC data will be used in the dashboard presentation but will not be ingested or retained beyond the Athena user's session:

- A-File Number;
- Name;
- Date of birth;
- Age;
- Gender;
- Whether the individual is part of a family group;
- Country of birth;
- Relevant health information;
- Any a law enforcement action taken;
- Sector/Station;
- Program name;
- Placement date;
- Placement time;
- Additional info; and
- Family group number.

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 these resources spend compiling statistics and analytics to support mission critical decisions responses to inquiries.

Key features of Qlik:

- Capturing and visualizing data through customizable dashboards
- Providing 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
- Presenting high-level information for decision makers in a graphical timeline and interactive geo-spatial views
- Identifying and analyzing specific causes of decreased performance