Privacy Impact Assessment
for the

Export Information System (EIS)

DHS/CBP/PIA-020

January 31, 2014

Contact Point
John Connors
Director, Import and Export Control, Office of Field Operations
U.S. Customs and Border Protection
(202) 325-3966

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

U.S. Customs and Border Protection (CBP) developed the Export Information System (EIS) to collect, use, and maintain paper and electronic records required to track, control, and process cargo exported from the United States. EIS serves to enhance national security, to enforce U.S. law (including those related to cargo safety and security, and smuggling), and to facilitate legitimate international trade. The exporting community must report to CBP export data that contains personally identifiable information (PII); therefore, CBP is publishing a privacy impact assessment (PIA) for EIS.

Overview

CBP protects the U.S. borders, and its mission is to safeguard the United States while fostering economic security through lawful international trade and travel. As part of its mission, CBP enforces export laws to enhance national security, to facilitate legitimate international trade to bolster the country's economy, and to strengthen the United States's ability to counter threats such as the proliferation of weapons of mass destruction. CBP created EIS as the central point through which export shipment data is accessed, as required by multiple federal agencies.

EIS includes information CBP collects from paper forms and documents, and via the Automated Export System and AESDirect (AES). EIS information that is from paper forms and documents is maintained in files at CBP ports and at headquarters. AES is an electronic database, jointly developed by CBP and the U.S. Census Bureau (Census) of the U.S. Department of Commerce.

Subsection (a) of section 343 of the Trade Act of 2002 mandated that the Secretary of Homeland Security (formerly the Secretary of Treasury) collect cargo information "through an electronic data interchange system," prior to the departure of the cargo from the United States by any mode of commercial transportation.[1] Pursuant to the statute, CBP promulgated a regulation requiring pre-departure filing of electronic information to allow CBP to examine the data before cargo leaves the United States.[2] To avoid redundancy, as specifically mandated by Congress, CBP required exporters to provide electronic cargo information through the existing system, AES. *See Mandatory Pre-Departure Filing of Export Cargo Information Through the Automated Export System*, 73 FR 32466 (June 9, 2008). Therefore, pursuant to the Trade Act of 2002,[3] AES presently acts, for exporters, as an electronic window through which both CBP collects its export information and Census collects Electronic Export Information (EEI)[4] for statistical purposes pursuant to 13 U.S.C. §§ 301-307.[5]

---

[1] *See* 19 U.S.C. § 2071 note.
[2] *See* 19 C.F.R. § 192.14.
[3] 19 U.S.C. § 2071 note, as implemented under 19 C.F.R. § 192.14.
[4] *Foreign Trade Regulations: Mandatory Automated Export System Filing for All Shipments Requiring Shipper's Export Declaration Information; Final Rule*, 73 FR 31548 (June 2, 2008). On September 30, 2008, CBP implemented its regulations requiring that CBP collect the mandatory, pre-departure export data through AES. *See Mandatory Pre-Departure Filing of Export Cargo Information Through the Automated Export System*, 73 FR 32466 (June 9, 2008).

DHS/CBP is issuing this privacy impact assessment to provide the public with information about how CBP is using EIS. CBP safeguards the records in EIS pursuant to all applicable system security and access policies, which include strict controls to minimize the risk of compromising the information in EIS. Only certain individuals, who have a need to know the information for the performance of their official duties, and who have also the requisite clearances and permissions, may have access to EIS. EIS interfaces with CBP's Automated Targeting System-Outbound (ATS-AT), which uses EIS information to conduct targeting and screening for high risk outbound cargo. This targeting and screening assists CBP officers in identifying exports with transportation safety and security risks, such as Office of Foreign Assets Control (OFAC)[6] violations, smuggled currency, illegal narcotics, and other contraband.[7] EIS information is used by the FALCON-Data Analysis & Research for Trade Transparency System (FALCON-DARTTS),[8] an U.S. Immigration and Customs Enforcement (ICE) system, to identify anomalous transactions that may indicate violations of U.S. trade laws.

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?

CBP has the authority to board vessels or vehicles and conduct searches of cargo pursuant to the Security and Accountability for Every (SAFE) Port Act of 2006, 19 U.S.C. §§ 482, 1467, 1581(a) and, Pub. L. 109-347, 120 Stat. 1884 (Oct. 13, 2006).

---

[5]Census has a statutory mandate to collect international trade statistics. *See Privacy Act of 1974; System of Records; Notice of New Privacy Act System of Records; Commerce/Census-12, Foreign Trade Statistics*, 74 FR 29676 (June 23, 2009) (Census system of records); *unchanged in Privacy Act of 1974; System of Records; Commerce/Census-12, Foreign Trade Statistics*, 74 FR 50780 (Oct.1, 2009) (announcing effective date as October 1, 2009). When it was initially deployed in 1995, AES served as a voluntary system for collecting the electronic equivalent of the paper Shipper's Export Declaration (SED) (U.S. Department of Commerce Form 7525-V), now known as EEI, which the legacy U.S. Customs Service transmitted to Census. Census collects export information for purposes of reporting statistics on international trade from the United States, pursuant to 13 U.S.C. §§ 301-307. AES now facilitates the collection of information that CBP maintains in EIS and uses to enforce and to improve compliance with U.S. export laws, pursuant to subsection (a) of section 343 of the Trade Act of 2002.

[6] U.S. Department of the Treasury OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy, or economy of the United States.

[7] Last PIA published- DHS/CBP/PIA-006(b) - Automated Targeting System (ATS) Update, June 1, 2012, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf.
SORN- DHS/CBP-006 - Automated Targeting System (May 22, 2012) 77 FR 30297, available at: http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm.

[8] Last PIA published - DHS/ICE/PIA-32(a) -FALCON-Data Analysis and Research for Trade Transparency System (FALCON-DARTTS) Update, January 16, 2014, available at: http://www.dhs.gov/publication/dhsicepia-032a-%E2%80%93-falcon-search-analysis-system-falcon-sa
SORN- DHS/ICE-005 - Trade Transparency Analysis and Research (TTAR) (September 4, 2012) 77 FR 53893, available at: https://www.federalregister.gov/articles/2012/09/04/2012-21691/privacy-act-of-1974-department-of-homeland-security-us-immigration-and-customs-enforcement-005-trade.

Vessels must obtain clearance from CBP prior to departing from the United States for a foreign port or place,[9] and pursuant to Tariff Act of 1930, as amended, CBP collects and reviews data for outbound cargo in EIS to ensure compliance with laws CBP is charged with enforcing.[10] Subsection (a) of section 343 of the Trade Act of 2002 mandated that the Secretary of Homeland Security (formerly the Secretary of Treasury) collect cargo information "through an electronic data interchange system," prior to the departure of the cargo from the United States. *See* 19 U.S.C. § 2071 note and 19 C.F.R. § 192.14. EIS includes the data collected via AES and AESDirect, and from paper forms and documents as CBP moves from paper to entirely electronic collection processes.

The export laws CBP enforces include, but are not limited to:

- The Tariff Act of 1930, as amended, 19 U.S.C. Chapter 4;
- 13 U.S.C. §§ 301-307 (Collection and Publication of Foreign Commerce and Trade Statistics) of 1962, Pub. L. 87-826, 76 Stat. 951, as amended;
- The Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today (PROTECT) Act of 2003, Pub. L. 108-21, 117 Stat. 650, as amended, 18 U.S.C. §§ 2251-2256; and 18 U.S.C. §§ 1461, 1463, 1465, and 1466 (relating to obscenity and child pornography);
- The Anti Car Theft Act of 1992, Pub. L. 102-519, 106 Stat. 3384, 19 U.S.C. §§ 1646b, 1646c;
- The Clean Diamond Trade Act (2003), Pub. L. 108-19, 117 Stat. 631, 19 U.S.C. §§ 3901-3913;
- The Federal Food, Drug and Cosmetic Act (1938), Pub. L. 75-717 , 52 Stat. 1040, as amended, 21 U.S.C. §§ 301-399;
- The Controlled Substances Import and Export Act (1970), Pub. L. 91-513, 84 Stat. 1236, as amended, 21 U.S.C. § 953;
- The Arms Export Control Act of 1979, Pub. L. 90-629, 82 Stat. 1320, as amended, 22 U.S.C. §§ 2778, 2780, and 2781;
- The Currency and Foreign Transactions Reporting Act of 1970 (commonly referred to as the Bank Secrecy Act), Pub. L. 91-508, 84 Stat. 1122, as amended, 31 U.S.C. § 5311, et seq.;
- The Atomic Energy Act of 1954, Pub. L. 83-703, 68 Stat. 919, as amended, 42 U.S.C. §§ 2011, 2077, 2122, 2131, 2138, 2155-2157;
- The Trading With the Enemy Act of 1917, Pub. L. 65-91, 40 Stat. 411, as amended, 50 U.S.C. App. §§ 1-44;
- The International Emergency Economic Powers Act (1977), Pub. L. 95-223, 91 Stat. 1628, as amended, 50 U.S.C. §§ 1701-1706;
- The Export Administration Regulations, 15 C.F.R. parts 730-744;

[9] *See* 46 U.S.C. § 60105.
[10] *See* 19 U.S.C. § 1431.

- The Lanham Act (Trademark Act of 1946), Pub. L. 79-489, 60 Stat. 427, as amended, 15 U.S.C. § 1051, et seq.; and
- The Endangered Species Act of 1973, Pub. L. 93-205, 87 Stat. 884, as amended, 16 U.S.C. § 1531, et seq.

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

CBP is publishing a SORN to cover EIS concurrently with this PIA.

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

No system security plan is warranted for the part of EIS that includes paper.

For the electronic system in EIS, the system security plan received its authority to operate (ATO) after it completed its certification and accreditation (C&A) on May 29, 2012, and is valid for three years.

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

CBP and NARA are reviewing the record retention and disposition schedule for EIS as part of CBP's SORN.

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

The PRA covers several groups of information collection in EIS:

- Shipper's Export Declaration (SED) Form 7525-V/Automated Export System (AES) Program, OMB Control No. 0607-0152, ICR Reference Nos. 200802-0607-001 and 201103-0607-010
- Transportation Manifest (Cargo Declaration), OMB Control No. 1651-0001, Information Collection Review (ICR) Reference No. 200710-1651-001, CBP Form 7509 and CBP Form 1302A
- Application for Exportation of Articles Under Special Bond, OMB Control No. 1651-0004, ICR Reference No. 201010-1651-001, CBP Form 3495
- Exportation of Self-Propelled Vehicles, OMB Control No. 1651-0054, ICR Reference No. 200907-1651-005
- General Declaration, OMB Control No. 1651-002, ICR Ref. No. 200906-1651-004, CBP Form 7507
- Certificate of Registration, OMB Control No. 1651-0010, ICR Ref. No. 200907-1651-001, CBP Form 4455 and 4457

Section 2.0 Characterization of the Information

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

EIS provides a central place into which export shipment data may be filed with CBP either on paper, or electronically via AES. EIS may collect and store the following PII related to the following categories of individuals:

- Filer or transmitter of information:
  - IRS number
  - Name
  - Address and zip code
  - Telephone number
  - Email address
- Exporter or U.S. Principal Party in Interest (USPPI):
  - IRS number
  - Name
  - Address and zip code
  - Telephone number
  - Export license, or other certificate, number
  - Department of State, Directorate of Defense Trade Controls Registration number

- Freight forwarder, or other U.S. authorized agent filing for the USPPI:
  - IRS number
  - Name
  - Address and zip code
  - Telephone number
  - Email address
- Shipper:
  - IRS number
  - Name
  - Address and zip code
  - Telephone number
- Intermediate consignee, who is the agent for the exporter in the foreign country:
  - Name
  - Address and zip code
  - Telephone number
- Ultimate Consignee, who is the person, party, or designee located abroad that will receive the export shipment:
  - Name
  - Address and zip code
  - Telephone number
- Individuals related to the specific commodity:[11]
  - Vehicle title number
  - Vehicle identification number (VIN)
  - Hazardous material emergency contact name and telephone number
  - License or certificate number
  - Certifier or License Registrant's number

[11] For example, if the merchandise is an item on the U.S. Munitions List or the Commerce Control List, AES will contain the Directorate of Defense Trade Controls (DDTC) license registrant's number, and may contain the items' serial numbers. If the exported merchandise is a used self-propelled vehicle, AES will contain the VIN and vehicle title number for that vehicle. The DDTC license registrant's number, serial numbers, the VIN, and the vehicle title number are necessary for the enforcement of specific export control laws.

- Serial number

EIS may contain Social Security Numbers (SSN) that were filed prior to December 3, 2009; however, at this time, EIS does not collect SSNs.[12]

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

EIS collects information primarily from exporters, USPPIs or their authorized U.S. agents, carriers, and freight forwarders. These parties may submit their data electronically using Census's web-based AESDirect, through third parties or services, or through a direct connection to CBP. Other filers submit paper documents directly to the port from which the cargo will depart.

EIS receives information from U.S. Department of State, Directorate of Defense Trade Controls (DDTC) containing an electronic version of most of the information on all DDTC-approved licenses for the export and temporary import of defense articles covered by the United States Munitions List. EIS receives information from the U.S. Department of Commerce, Bureau of Industry and Security (BIS) to confirm BIS-licensed shipments for exports and re-exports that are covered by the Export Administration Regulations.[13] In addition, for merchandise that could not be covered by an electronic license, EIS collects paper copies of DDTC and BIS licenses. For certain exports of used, self-propelled vehicles that CBP officials have selected to examine, EIS receives the VINs of stolen automobiles from the National Crime Information Center (NCIC) of the Federal Bureau of Investigation (FBI).

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. EIS does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

To ensure accuracy, CBP officials collect data directly from the exporters. CBP officials review the data in EIS, and may verify it by inspecting the cargo and accompanying documentation. For electronic information, filers must receive training from CBP, and obtain a certification from CBP before transmitting data. When the filer is authorized to transmit data, the system validates each data transmission. After certification, CBP and Census require the filer to maintain an acceptable level of performance filing timely and accurate information into AES (and thus EIS) electronic filings. Once

[12] Foreign Trade Regulations (FTR): Eliminate the Social Security Number (SSN) as an Identification Number in the Automated Export System (AES); Interim Final Rule, 74 FR 38914 (Aug. 5, 2009)

[13] *See* 15 C.F.R. § 730.3 (describing covered merchandise as including "purely civilian items, items with both civil and military, terrorism or potential WMD-related [weapons of mass destruction-related] applications, and items that are exclusively used for military applications but that do not warrant control under the International Traffic in Arms Regulations.")

electronic data has been accepted into EIS, AES generates and returns an Internal Transaction Number (ITN) as confirmation of successful electronic filing.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: EIS contains more personal information than is necessary track, control, and process cargo exported from the United States.

Mitigation: The data in EIS are limited to information relevant and necessary for export control enforcement and international trade statistics. Name, address, telephone number, and other contact and identifying information associated with exported cargo are needed to identify individuals associated with exported cargo, and to identify individuals who violate export laws. For example, the names of the shipper, USPPI, intermediate consignee, and the ultimate consignee, are necessary to ensure that merchandise is not sold to unauthorized end users. The license registrant's number and the license number itself ensures that the covered merchandise is being exported legally. A used self-propelled vehicle's title number and VIN are necessary to ensure that the automobile has not been stolen.

As an example of CBP's efforts to minimize the PII collected to only that which is necessary, CBP's paper export forms do not require SSNs. Although AES used SSNs for identification purposes when it was first deployed in 1995, it no longer collects SSNs and is in the process of removing all SSNs from the database. EIS only maintains SSNs to the extent previously collected as a result of prior AES policies. The SSNs will be archived after five years and deleted after an additional ten years, in conformance with the EIS retention procedures.

Privacy Risk: If data is entered inaccurately into AES or AESDirect EIS could contain inaccurate information about individuals.

Mitigation: Every individual, whether she is herself the USPPI; an employee of an exporter, USPPI, freight forwarder, or shipper; or a U.S. agent authorized to file on behalf of a USPPI; must complete training and be certified before he or she may transmit any information into AES or AESDirect. AES contains parameters that will alert the individual who entered the information into AES or AESDirect if the information they submit is inaccurate or otherwise inadequate. Individuals may enter the information themselves, and may correct or amend it. If an exporter uses an agent or a service center to file its information, that third party must have written authorization from the exporter and have AES certification.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

CBP uses information in EIS to collect, use, and maintain paper and electronic records required to track, control, and process cargo exported from the United States. EIS serves to enhance national security, to enforce U.S. law, and to facilitate legitimate international trade, including detecting and preventing the export of certain items by unauthorized parties to unauthorized destinations or end users and other possible violations of export laws.

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. EIS does not identify or locate predictive patterns, and the results of any analyses conducted by other systems do not appear in EIS. However, EIS interfaces with the ATS-AT, which uses EIS information to conduct targeting and screening for high risk outbound cargo. This targeting and screening assists CBP officers in identifying exports with transportation safety and security risks, such as OFAC violations, smuggled currency, illegal narcotics, and other contraband. EIS information is also used by ICE's FALCON-DARTTS to identify anomalous transactions that may indicate violations of U.S. trade laws. However, the results of any analyses conducted by other DHS systems do not appear in EIS.

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

CBP also shares EIS data, within DHS, with FALCON-DARTTS to assist ICE with the investigation of trade-based money laundering, contraband smuggling, and trade fraud. EIS sends batches of data directly to the FALCON-DARTTS mainframe platform, and officials from the ICE Homeland Security Investigations, which owns FALCON-DARTTS, load the data into FALCON-DARTTS. ICE officials, who have access to ATS, have access to EIS information transmitted to ATS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: Unauthorized use of information in EIS by external users (filers) or internal users (CBP employees) of the system.

Mitigation: Although certified AES filers may transmit data to AES or AESDirect, they do not have access to query AES or EIS.

CBP officials must complete privacy training, and must obtain approval from their supervisors to access EIS. CBP maintains the paper documents and records, and the electronic information in EIS in controlled spaces protected by armed individuals. CBP tracks the electronic information search activities of its users, and provides audit logs, which CBP security officials review. Any inappropriate use of EIS results in an investigation and suspension of the user's access to EIS, and may result in further disciplinary or criminal investigation.

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.

CBP has provided notice of the scope of information collected in EIS through publications in the Federal Register,[14] information on the public CBP website,[15] and this PIA.

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

U.S. law requires shippers and exporters to provide CBP information that contains personally identifiable information. When shippers or exporters submit the required information to EIS, in a paper format or via AES or AESDirect, they fulfill their legal requirements, and they consent to how CBP will properly use the data.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not know that their information is collected in EIS.

Mitigation: CBP has provided notice of the scope of information collected in EIS through publications in the Federal Register[16] and information on the public CBP website.[17] To increase transparency, CBP is publishing the EIS SORN and this PIA.

---

[14] The publications include *Required Advance Electronic Presentation of Cargo Information; Final Rule*, 68 FR 68140 (December 5, 2003); *Importer Security Filing and Additional Carrier Requirements; Interim Final Rule*, 73 FR 71730 (November 25, 2008); *Technical Correction To Remove Obsolete Compliance Date Provisions From Electronic Cargo Information Regulations; Final Rule*, 74 FR 52675 (October 14, 2009); *Dec. 10-29; Technical Corrections to Customs and Border Protection Regulations*; *Final Rule*, 75 FR 52438 (August 26, 2010).

[15] http://www.cbp.gov/xp/cgov/trade/basic_trade/export_docs/, http://www.cbp.gov/xp/cgov/trade/trade_outreach/advance_info/, and http://www.cbp.gov/xp/cgov/trade/automated/aes/

[16] *See Required Advance Electronic Presentation of Cargo Information; Final Rule*, 68 FR 68140 (December 5, 2003).

[17] http://www.cbp.gov/xp/cgov/trade/basic_trade/export_docs/, http://www.cbp.gov/xp/cgov/trade/trade_outreach/advance_info/, and http://www.cbp.gov/xp/cgov/trade/automated/aes/

Section 5.0 Data Retention by the project

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

CBP retains EIS data in an active status for five years. After five years, CBP will archive the data it for an additional ten years. CBP will retain, beyond fifteen years, specific EIS data needed for the duration of a law enforcement investigation or judicial proceeding, when the investigation or proceeding continues beyond fifteen years.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: EIS may retain the data for an unnecessary length of time.

Mitigation: CBP keeps EIS data, paper and electronic, in an active status for five years, to align with the Foreign Trade Regulations, in 15 C.F.R. Part 30, which require that parties maintain records, and have the ability to correct transmissions to AES, for five years. After five years, CBP will archive EIS data for an additional ten years, to align with the requirements of other U.S. government agencies for licensed shipments, or for law enforcement purposes. As noted above, CBP will retain, beyond fifteen years, specific EIS data needed for the duration of a law enforcement investigation or judicial proceeding, when the investigation or proceeding continues beyond fifteen years.

Section 6.0 Information Sharing

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

CBP transmits EIS data through AES to Census, so that Census may fulfill its statutorily mandated requirements to collect and publish foreign commerce and trade statistics. *See* 13 U.S.C. §§ 301-307.

As required by 19 U.S.C. § 1431, 46, U.S.C. § 60105, and 19 C.F.R. § 103.31, certain outbound manifest data in EIS may be made available for publication; however, no commercial or financial information, such as the names of the consignees, is included in any disclosure to the public. A shipper may request that his or her name and address be treated as confidential, pursuant to 19 C.F.R. § 103.31(d)(2).

Pursuant to the Anti-Car Theft Act of 1992, CBP checks the VIN of used automobiles that are to be exported from the United States against the NCIC, and CBP provides the FBI the VINs in the event there is a match to an NCIC record indicating the car was reported stolen. *See* 19 U.S.C. § 1646c.

CBP may disclose EIS information on a case-by-case basis, consistent with the routine uses explained in the EIS System of Records Notice, which CBP is publishing contemporaneously with this PIA.

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

Routine use H allows CBP to transmit EIS data to Census, so that Census may fulfill its statutorily mandated requirements to collect international trade statistics. Routine use I allows CBP to transmit information to NCIC and the FBI, so that CBP and the FBI may enforce the Anti Car Theft Act of 1992. Routine use R allows CBP to transmit certain outbound manifest information to the public, pursuant to 19 U.S.C. § 1431, 46 U.S.C. § 60105, and 19 C.F.R. § 103.31.

To ensure cargo safety and security, or to prevent smuggling, CBP will disclose EIS information only on a case-by-case basis to entities for specific uses, which include export control, anti-terrorism, international trade statistics, and law enforcement.

6.3 Does the project place limitations on re-dissemination?

Yes. As a condition of sharing information pursuant to a routine use in the EIS SORN, CBP requires anyone who receives non-public EIS data to obtain written permission from CBP before re-disseminating the information.

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

To obtain EIS information, the requesting party must make the request in writing, describing the specific information it requests and specifically how it will use the information, which must be related to export control, international trade statistics, or law enforcement. CBP retains a copy of this request, which an official in the CBP Privacy Office reviews. For requests that the CBP Privacy Office reviews, on a case-by-case basis the CBP Privacy Office official then drafts an authorization memorandum specific to each case, and CBP retains the memorandum. If the disclosure is approved, CBP also maintains a record of the disclosure. Other requests may be covered by a memorandum of understanding, which memorializes regular sharing.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk that CBP could share data outside DHS for purposes that differ from the stated purpose and use of the original collection, and that external agencies could further disseminate the information.

Mitigation: These risks are minimal because disclosure is permitted only upon authorization and in accordance with the routine uses in the EIS SORN. As DHS procedures and policies require, all current external sharing arrangements, whether on a case-by-case basis or pursuant to a memorandum of understanding, are compatible with the original purpose of the collection. The CBP Privacy Office reviews specific requests for EIS data. The CBP Privacy Officer issues an authorization memorandum when he or she determines CBP may share that particular information based on the routine uses in the EIS SORN or other statutory authority. All authorization memoranda expressly forbid the sharing of information to third parties, unless CBP authorizes the sharing or the individual consents to the sharing.

All CBP memoranda of understanding require that the agency receiving CBP information agree to obtain authorization from CBP before sharing information to third parties.

Section 7.0 Redress

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

As described in section 6.1 and 6.2 of this PIA, certain outbound manifest information in EIS is made available to the public. Information from paper documents will be made available to individuals pursuant to an approved request, as described in the next paragraph. Individuals who have filed their information electronically cannot conduct queries in AES of their electronic submissions; however, their own software allows them to review what they transmitted into AES, before AES accepted it.

To gain access to non-public information in EIS, an individual may request information about his or her EIS records, pursuant to procedures provided by the Freedom of Information Act (FOIA) (5 U.S.C. § 552) and the access provisions of the Privacy Act of 1974 (5 U.S.C. § 552a(d)), and by writing to:

U.S. Customs and Border Protection (CBP)

Freedom of Information Act (FOIA) Division

90 K Street NE

Washington, DC 20229

When seeking records from EIS or any other CBP system of records, the request must conform to Part 5, Title 6 of the Code of Federal Regulations. *See* 6 C.F.R. Part 5. An individual must provide his or her full name, current address, and date and place of birth. He or she must also provide:

- An explanation of why the individual believes DHS would have information on him or her;
- Details outlining when he or 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.

The request must include a notarized signature or be submitted pursuant to 28 U.S.C. § 1746, which permits statements to be made under penalty of perjury as a substitute for notarization. Without this 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. Although CBP does not require a specific form, guidance for filing a request for information is available on the DHS website at http://www.dhs.gov/file-privacy-act-request and at http://www.dhs.gov/file-foia-overview.

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

Individuals who file information electronically may amend, correct, or cancel their active data, and those changes are reflected through updates in EIS. When their data is cancelled, it is removed from

EIS. Filers may also contact their individual Census (for AES) and CBP (for EIS) client representatives, or the Census AES Branch Helpdesk.[18] Individuals may also contact the CBP INFO Center, to request correction of erroneous EIS information. *See* section 7.1, above.

While certain outbound manifest information must generally be made available for publication, shippers may request that CBP hold their names, addresses, and tax identifying number (TIN) in confidence by submitting a certification claiming confidential treatment. Such certifications allow businesses and individuals to partially shield their identity from association with their exports in these publications while still permitting CBP to screen their exports. Approved certifications are valid for two years after the approval date.[19] Shippers may submit a letter via email (vesselmanifestconfidentiality@cbp.dhs.gov), by Fax (202) 325-0154, or by mail (address below) to CBP requesting that their company name not be disclosed on the vessel manifest. There is no fee associated with the request for confidentiality.[20]

CBP Privacy Officer
U.S. Customs and Border Protection
90 K Street, N.E.
10th Floor
Washington D.C. 20229-1177

Individuals may notify CBP that they believe their information in EIS is incorrect or inaccurate, and may send their requests for correction to:

U.S. Customs and Border Protection
CBP INFO Center
Office of Public Affairs
1300 Pennsylvania Avenue
Washington, DC 20229

Although requests to amend information should be made in writing, individuals may contact the CBP INFO Center by phone at (877) 227-5511 or (703) 526-4200. Following the links on https://help.cbp.gov/app/home/search/1, individuals may submit complaints online.

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

Individuals may contact the CBP INFO Center to obtain guidance for requesting correction of their EIS information; this PIA and www.cbp.gov provide contact information for making those requests. Within EIS, individuals who submit information electronically are notified of the procedures for

---

[18] Individuals may contact the Census AES Helpdesk by telephone, at (800) 549-0595, by email at askAES@Census.gov, or online on its website at http://www.census.gov/foreign-trade/feedback/index.html

[19] *See* 19 C.F.R. § 103.31(d)(2). "Confidential treatment", pursuant to 19 C.F.R. § 103.31(d)(2), means that CBP will not disclose the information to the public. It does not refer to the national security classification.

[20] Further information available at: https://help.cbp.gov/app/answers/detail/a_id/285/~/importers---confidential-treatment-of-vessel-manifest-data.

correcting their information in the electronic user guides and during the electronic filer certification process.[21] Furthermore, when the electronic system encounters a possible error with the transmitted data, it will issue a response message alerting the filer that it may need to correct the information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: A potential risk related to redress occurs with the ability to validate the accuracy of third-party information, because EIS contains PII that pertains to third parties, such as the ultimate consignee name, serial numbers, and VIN numbers.

Mitigation: Individuals and third parties, including those who submit information in hard copy format, may contact CBP when they believe that the data contained in EIS is inaccurate. Individuals who file electronically may submit corrections electronically, and filers must meet standards of quality, accuracy, and timeliness to be allowed to transmit data to EIS.

Section 8.0 Auditing and Accountability

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

CBP officials may obtain access to EIS only on a "need to know basis" and after their supervisor and the EIS business owner has authorized their access. For the paper records, only CBP officials authorized to review EIS may obtain access to them. Authorized EIS users may obtain electronic access through the CBP network through encrypted passwords and sign-on identification. EIS records who logged into the system, what functions were performed, when, and what changes were made, if any. CBP reviews audit logs, and conducts periodic reviews of the users.

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

CBP EIS users are required to take the annual privacy and security training such as the "CBP IT Security Incident Response Training," "CBP IT Security Awareness and Rules of Behavior Training," "CBP Safeguarding Classified National Security Information," "CBP Sensitive Security Information" through the online DHS – Virtual Learning Center. Each of these courses covers how CBP EIS users must handle PII.

The EIS program manager maintains a master list of all EIS users, and when they have taken privacy and security training. If an EIS user fails to complete the training by the annual deadline, then he or she loses access to EIS.

---

[21] User guides are available online at http://www.aesdirect.gov/support/userguide.html and http://www.cbp.gov/xp/cgov/trade/automated/aes/

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

A CBP official's supervisor must request that an individual CBP official have access to EIS, and the supervisor submits the request to the EIS program manager. Both the CBP official's supervisor and the EIS program manager determine whether the particular CBP official has a "need to know" basis for access to EIS. After approval from the program manager, the supervisor transmits the request to the Security Help Desk, which determines whether the CBP official has completed the necessary background investigation. If the CBP official does not use EIS for 90 days, or if the CBP official's profile changes, then he or she must again obtain authorization from his or her supervisor, EIS program manager, and the Security Help Desk to obtain access to EIS. After the CBP official has obtained all the necessary approval, then the electronic system in EIS will accept the CBP official's specific user sign-on identification and password. Also the CBP official will have access to the paper files, by showing his or her photo identification.

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?

For new sharing agreements and authorizations for access to any EIS information, the agency, component, or organization must obtain a written agreement or written authorization from CBP. The CBP Privacy Officer reviews all such agreements and authorizations.

Responsible Officials

John Connors
Director, Import and Export Control,
Office of Field Operations
U.S. Customs and Border Protection

Laurence Castelli
CBP Privacy Officer
U.S. Customs and Border Protection
(202) 344-1610

Approval Signature

Original signed and on file with the DHS Privacy Office

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security