9111-14

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2015-0054]

Privacy Act of 1974; Department of Homeland Security U.S. Customs and Border Protection-DHS/CBP-020 Export Information System (EIS) System of Records.

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to issue a new Department of Homeland Security system of records titled, "Department of Homeland Security/U.S. Customs and Border Protection - DHS/CBP-020 Export Information System System of Records." This system of records is used by the Department of Homeland Security/U.S. Customs and Border Protection to collect and maintain records on export commodity and transportation shipment data. Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act of 1974, as amended, elsewhere in the Federal Register. This system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF

PUBLICATION IN THE FEDERAL REGISTER]. This new system will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2015-0054 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Karen L. Neuman, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

INSTRUCTIONS: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

DOCKET: For access to the docket to read background documents or comments received, please visit http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: John Connors (202-344-1610), CBP Privacy Officer, U.S. Customs and Border Protection, Department of Homeland Security, Washington, D.C. 20229. For privacy questions, please contact: Karen L. Neuman (202-343-1717), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) proposes to establish a new DHS system of records titled, "DHS/CBP-020 Export Information System (EIS) System of Records." The system of records is used by CBP to collect, use, and maintain paper and electronic records required to track, control, and process cargo exported from the United States. EIS allows CBP to enhance national security, enforce U.S. law, and facilitate legitimate international trade.

CBP is publishing a system of records notice (SORN) for EIS because CBP uses EIS to collect and process information to comply with export laws and facilitate legitimate international trade. CBP is charged with enforcing all U.S. export laws at the border and the exporting community is required to report export data to CBP that contains personally identifiable information (PII).

Subsection (a) of Section 343 of the Trade Act of 2002 (19 U.S.C. 2071) mandates 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 (*see* 19 U.S.C. 2071 note.) Pursuant to 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 (*see Electronic Information for Outward Cargo Required in Advance of Departure* (19 C.F.R. 192.14)). CBP required exporters to provide electronic cargo information through the Automated Export System (AES) to avoid redundancy as specifically mandated by Congress (*see Mandatory Pre-Departure Filing*

of Export Cargo Information Through the Automated Export System, 73 Fed. Reg. 32466 (June 9, 2008)).

To comply with the regulation, exporters must file the Electronic Export Information (EEI), formerly the Shipper's Export Declaration (SED)[1] when the value of the commodity classified under each individual Schedule B number is over $2,500 or if a validated export license is required to export the commodity. The exporter is responsible for preparing the EEI and the carrier files it with CBP through the AES or AES Direct (operated by the Department of Commerce, U.S. Census Bureau). Cargo information collected by CBP includes PII such as a shipper's name, address, and tax identifying number (TIN).

According to the U.S. Census Bureau, in a standard export transaction, it is the U.S. Principal Party in Interest's (USPPI) responsibility to prepare the EEI. However, the USPPI can give freight forwarders a power of attorney (POA) or written statement (WA) authorizing them to prepare and file the EEI on their behalf. In a routed export transaction, however, the Foreign Principal Party in Interest (FPPI) must provide a POA or WA to prepare the EEI to either the USPPI or a U.S. Authorized Agent.

The Internal Transaction Number (ITN) or exemption citation must be provided by the EEI filer to the carrier when the goods are presented for export. The carrier is responsible for providing the ITN or exemption citation to CBP. CBP Officers will

[1] 13 U.S.C. 301 (Department of Commerce, U.S. Census Bureau root authority to collect the SED, now EEI); pursuant to section 303, CBP (then U.S. Customs Service, Dept. of Treasury) is required to develop an automated system for collecting this export data. Through title 13, the Census Bureau holds stewardship of export data. Under the Trade Act of 2002 (19 U.S.C. 2071 note), CBP is required to collect an export manifest containing a declaration identifying the parties to the transaction, a physical description of the commodity, its quantity, mode of conveyance, and ports of origin and destination. Through title 19, CBP, similarly, holds stewardship of export data.

verify that the ITN or exemption citations clearly stated on export documents and provided to the carrier(s) within the prescribed timeframes. The procedures for filing vary by cargo type (vessel, truck, air, or rail). The timeframes for filing varies according to the method of transportation for pre-departure filing (State Department United States Munitions List (USML) shipments and non-USML shipments).

CBP is publishing this system of records notice to provide notice of the records maintained by CBP concerning individuals who participate in exporting goods from the United States. CBP previously published a Privacy Impact Assessment (PIA) for EIS last year.[2]

Consistent with DHS's information-sharing mission, information stored in the DHS/CBP-020 EIS System of Records may be shared with other DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, information may be shared with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies or other parties consistent with the routine uses set forth in this SORN. In particular, information may be shared with the U.S. Department of Commerce, Bureau of Industry and Security, and the U.S. Department of State, Directorate of Defense Trade Controls, relating to compliance and enforcement of licenses issued by these respective agencies concerning the controlled nature or sensitive technology present in the exported commodities (e.g., certain central processing unit designs, weapons systems).

[2] http://www.dhs.gov/publication/export-information-system-eis

Additionally, DHS is issuing a Notice of Proposed Rulemaking elsewhere in the Federal Register to exempt this system of records from certain provisions of the Privacy Act. This system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework that govern the means by which federal agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. An individual is defined in the Privacy Act to encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all persons when systems of records maintain information on U.S. citizens, lawful permanent residents, and foreign nationals.

Below is the description of the DHS/CBP-020 EIS System of Records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

System of Records

Department of Homeland Security (DHS)/ U.S. Customs and Border Protection (CBP)-020

System name:

DHS/CBP-020 Export Information System (EIS) System.

Security classification:

Unclassified.

System location:

Records are maintained at the CBP Headquarters in Washington, D.C., and field offices.

Categories of individuals covered by the system:

The categories of individuals covered by the system are DHS or CBP employees and individuals who process and ensure the compliance of goods exported from the United States. Those individuals who process and ensure the compliance of exported goods include: the filer or transmitter of the information; the exporter or U.S. Principal Party in Interest (USPPI); the freight forwarder, or other U.S. authorized agent filing for the USPPI; the shipper; the intermediate consignee, who is the agent for the exporter in the foreign country; the ultimate consignee, who is the person, party, or designee located abroad that will receive the export shipment; and individuals related to the specific commodity (e.g., for hazardous material, an emergency point of contact).

Categories of records in the system:

EIS contains records that include the following information:

- Information about the filer, exporter, USPPI, ultimate consignee, or authorized U.S. agent, which may include:
    - Full name;
    - Tax Identification Number (TIN) or other trade identifiers;
    - Telephone numbers;

    - Email addresses;
    - Addresses and zip codes;
    - Certificate or license numbers (including licenses issued by various federal agencies);
    - Signatures; and
    - License certifier or other registration numbers.
- Information about the DHS/CBP employee annotating the record or ensuring compliance with export control regulations, which may include:
    - Full Name;
    - Identification number or badge number.
- Shipment information:
    - Mode of transportation;
    - Carrier;
    - Origin, port of export, port of unlading, and destination;
    - Date of export; and
    - Hazardous material indicator.
- Commodity information:
    - Description, which may include the make, model, serial number, caliber, manufacturer, or hazardous material description;
    - Quantity;
    - Value;
    - Weight;

- License, certification document, export license, or Kimberly Process Certificate numbers;[3]
- Vehicle title numbers;
- Vehicle identification number (VIN);
- Certificate or license registrant's number; and
- Hazardous material emergency contact name and telephone number.

Authority for maintenance of the system:

Pursuant to 19 U.S.C. 482, 1467, 1581(a) and the Security and Accountability for Every (SAFE) Port Act of 2006, Pub. L. 109-347, 120 Stat. 1884 (Oct. 13, 2006); CBP has the authority to board vessels or vehicles and conduct searches of cargo; pursuant to 46 U.S.C. 60105, vessels must obtain clearance from CBP prior to departing from the United States for a foreign port or place; and pursuant to 19 U.S.C. 1431, CBP collects and reviews data for outbound cargo in EIS to ensure compliance with laws CBP is charged with enforcing. 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 in AES/ACE and from paper forms and documents, as CBP moves from paper to an entirely electronic collection process.

The export laws CBP enforces include:

[3]A Kimberly Process Certificate number is a control number issued on each Kimberly Diamond Process certificate pursuant to the Clean Diamond Trade Act (2003), Pub. L. 108-19, 117 Stat. 631, 19 U.S.C. 3901-3913.

- 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
- 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.

Purpose(s):

The purpose of EIS is to be the central point through which CBP collects and maintains export data and related records to facilitate DHS's law enforcement and border security missions. DHS uses EIS as a tool to further its mission to ensure the safety and security of cargo, prevent smuggling, and enforce export and other applicable U.S. laws.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

Consistent with the purposes noted above, or as otherwise authorized by law, and in addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including Offices of the U.S. Attorney, or other federal agency conducting litigation or in proceedings before any court,

adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any Component thereof;

2. Any employee or former employee of DHS in his or her official capacity;

3. Any employee or former employee of DHS in his or her individual capacity when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made pursuant to a written Privacy Act waiver at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. DHS has determined that as a result of the suspected or confirmed compromise, there is a risk of identity theft or fraud, harm to economic or property interests, harm to an individual, or harm to the security or integrity of this system or other

systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals who are provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing a statute, rule, regulation, order, license, or treaty when DHS believes the information would assist the enforcement of civil or criminal laws.

H. To the Department of Commerce, U.S. Census Bureau to fulfill its statutory mandate of collecting international trade statistics.

I. To federal agencies, pursuant to the International Trade Data System Memorandum of Understanding, consistent with the receiving agency's legal authority to collect information pertaining to or regulating transactions to ensure cargo safety and security, or to prevent smuggling.

J. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations when DHS reasonably believes there to be a threat or potential threat to national or international security and for which the information may be relevant in countering the threat or potential threat.

K. To a federal, state, tribal, or local agency, or other appropriate entity or individual, or foreign governments, in order to provide relevant information related to intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

L. To an organization or individual in either the public or private sector, either foreign or domestic, when there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, or when the information is relevant and necessary to the protection of life or property.

M. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations, in response to a subpoena, or in connection with criminal law proceedings;

N. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation.

O. To a former employee of DHS, in accordance with applicable regulations, for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes when

DHS requires information or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

P. To an appropriate federal, state, local, tribal, foreign, or international agency, if the information is relevant to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit.

Q. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital health interests of a data subject or other persons (e.g., to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats). Appropriate notice will be provided of any identified health threat or risk.

R. To the public, certain outbound manifest information, including the name and address of the shipper; general character, size, weight, and description of the cargo; the name of the vessel or carrier; the port of exit; the port of destination; and country of destination; and which may be made public pursuant to 19 U.S.C. 1431, 46 U.S.C. 60105, and 19 C.F.R. 103.31.

S. To organizations engaged in theft prevention activities regarding certain outbound manifest information regarding vehicles, as authorized pursuant to 19 U.S.C.

1627a.

T. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

CBP stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, digital media, and CD-ROM.

Retrievability:

CBP retrieves records by name, address, telephone number, search terms, or TIN.

Safeguards:

CBP safeguards records in this system in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. CBP imposes strict controls to minimize the risk of compromising the information it

stores. CBP limits access to the computer system containing the records in this system to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

Retention and disposal:

CBP retains EIS data, including AES/ACE data, in an active status for five years. The data is retained for an additional ten years to meet any requirements of a controlling U.S. Government agency for licensed shipments or for law enforcement purposes. The data is archived after five years and deleted after the additional ten year period, in conformance with the EIS retention procedures. CBP retains information beyond fifteen years when specific EIS data is needed for the duration of a law enforcement investigation or judicial proceeding, when the investigation or proceeding continues beyond fifteen years.

System Manager and address:

Chief, Export Control Branch, Office of Field Operations, U.S. Customs and Border Protection Headquarters, 1300 Pennsylvania Avenue NW, Washington, D.C. 20229.

Notification procedure:

The Secretary of Homeland Security has exempted this system from the notification, access, accounting, and amendment procedures of the Privacy Act because it is a law enforcement system. However, DHS/CBP will consider individual requests to determine whether or not information may be released. Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its

content, may submit a request in writing to the Headquarters or component's Freedom of Information Act Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief FOIA Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0655, Washington, D.C. 20528.

When individuals seek records about themselves from this system of records or any other Departmental system of records, their requests must conform with the Privacy Act regulations set forth in 6 C.F.R. Part 5. They must first verify their identities, meaning that they must provide their full names, current addresses, and dates and places of birth. They must sign their requests, and each of their signatures must either be notarized 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, they may obtain forms for this purpose from the Chief Privacy Officer and Chief FOIA Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, they should:

- Explain why the Department would have information about them;
- Identify which component(s) of the Department would have the information;
- Specify when the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

If the individuals' requests seek records pertaining to another living person, they must include a statement from that individual certifying his/her agreement for them to have access to his/her records.

Without the above information the component(s) may not be able to conduct an effective search and a request may be denied due to lack of specificity or lack of compliance with applicable regulations.

Record access procedures:

See "Notification procedure" above.

Contesting record procedures:

See "Notification procedure" above.

Record source categories:

CBP obtains records from individuals who participate in exporting goods from the United States and other federal agencies, as required to administer the export laws of the United States.

Exemptions claimed for the system:

DHS/CBP is not requesting an exemption with respect to information maintained in the system as it relates to data submitted by or on behalf of an individual. Information in the system may be shared pursuant to the exceptions under the Privacy Act (5 U.S.C. 552a(b)) and the above routine uses. The Privacy Act requires DHS to maintain an accounting of the disclosures made pursuant to all routines uses. Disclosing the fact that a law enforcement or intelligence agency has sought particular records may affect ongoing law enforcement activity. Therefore, pursuant to 5 U.S.C. 552a(j)(2), DHS will claim

exemption from sections (c)(3), (e)(8), and (g)(1) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information. In addition, pursuant to 5 U.S.C. § 552a(k)(2), DHS will claim exemption from section (c)(3) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information.

Dated: August 19, 2015.

Karen L. Neuman

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2015-21675 Filed: 9/1/2015 08:45 am; Publication Date: 9/2/2015]