9110-06

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2011-0113]

Privacy Act of 1974; Department of Homeland Security, U.S. Customs and Border Protection, DHS/CBP—017 Analytical Framework for Intelligence (AFI) System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to establish a new Department of Homeland Security system of records titled, "Department of Homeland Security, U.S. Customs and Border Protection, DHS/CBP—017 Analytical Framework for Intelligence (AFI) System of Records." This system of records will allow the Department of Homeland Security/U.S. Customs and Border Protection to improve border and national security by providing AFI users with a single platform for research, analysis, and visualization of large amounts of data from disparate sources and maintaining the final analysis or products in a single, searchable location for later use as well as appropriate dissemination. Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking concurrent with this system of records elsewhere in the Federal Register. This newly established 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 PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2011-0113 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 703-483-2999.
- Mail: Mary Ellen Callahan, 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 go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Laurence E. Castelli (202-325-0280), CBP Privacy Officer, Office of International Trade, U.S. Customs and Border Protection, Mint Annex, 799 Ninth Street, NW, Washington, D.C. 20229. For privacy issues please contact: Mary Ellen Callahan (703-235-0780), 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/ U.S. Customs and Border Protection, DHS/CBP—017 Analytical Framework for Intelligence (AFI) System of Records." CBP is publishing this SORN because AFI is a group of records under the control of CBP that contains personally identifiable information which is retrieved by a unique identifier.

AFI enhances DHS's ability to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk; and it aids in the enforcement of customs and immigration laws, and other laws enforced by DHS at the border. AFI is used for the purposes of: 1) identifying individuals, associations, or relationships that may pose a potential law enforcement or security risk, targeting cargo that may present a threat, and assisting intelligence product users in the field in preventing the illegal entry of people and goods, or identifying other violations of law; 2) conducting additional research on persons and/or cargo to understand whether there are patterns or trends that could assist in the identification of potential law enforcement or security risks; and 3) sharing finished intelligence products developed in connection with the above purposes with DHS employees who have a need to know the analysis in the intelligence products in the performance of their official duties and who have appropriate clearances or permissions. Finished intelligence products are tactical, operational, and strategic law enforcement intelligence products that have been reviewed and approved for sharing with finished intelligence product users and authorities outside of DHS, pursuant to routine uses.

To support its capability to efficiently query multiple data sources, AFI creates and maintains an index, which is a portion of the necessary and relevant data in existing operational DHS source systems, by ingesting this data through and from the Automated Targeting System (ATS) and other source systems. In addition to the index, AFI provides AFI analysts with different tools that assist in detecting trends, patterns, and emerging threats, and in identifying non-obvious relationships.

AFI improves the efficiency and effectiveness of CBP's research and analysis process by providing a platform for the research, collaboration, approval, and publication of finished intelligence products.

AFI provides a platform for preparing responses to requests for information (RFIs). AFI will centrally maintain the requests, the research based on those requests, and the response to those requests. AFI allows analysts to perform federated queries against external systems of record, including those of Department of State, the Department of Justice/FBI, as well as publicly and commercially available data sources, and eventually, classified data. AFI also enables an authorized user to search the Internet for additional information that may contribute to an intelligence gathering and analysis effort. AFI facilitates the sharing of finished intelligence products within DHS and tracks sharing outside of DHS.

Two principal types of users will access AFI: DHS analysts and DHS finished intelligence product users. Analysts will use the system to obtain a more comprehensive view of data available to CBP, and then analyze and interpret that data using the visualization and collaboration tools accessible in AFI. If an analyst finds actionable terrorist, law enforcement, or intelligence information, he may use relevant information

to produce a report, create an alert, or take some other appropriate action within DHS's mission and authorities. In addition to using AFI as a workspace to analyze and interpret data, analysts may submit or respond to RFIs, assign tasks, or create finished intelligence products based on their research or in response to an RFI. Finished intelligence product users are officers, agents, and employees of DHS who have been determined to have a need to know the analysis in the intelligence products in the performance of their official duties and who have appropriate clearances or permissions. Finished intelligence product users will have more limited access to AFI, will not have access to the research space or tools, and will only view finished intelligence products that analysts published in AFI. Finished intelligence product users are not able to query the data from the source systems through AFI.

AFI performs extensive auditing that records the search activities of all users to mitigate any risk of authorized users conducting searches for inappropriate purposes. AFI also requires that analysts re-certify annually any user-provided information marked as containing PII to ensure its continued relevance and accuracy. Analysts will be prompted to re-certify any documents that contain PII which are not related to a finished intelligence product. Information that is not re-certified is automatically purged from AFI. Account access is controlled by AFI passing individual user credentials to the originating system or through a previously approved certification process in another system in order to minimize the risk of unauthorized access. When an analyst conducts a search for products, AFI will only display those results that an individual user has permission to view.

Consistent with DHS's information sharing mission, information stored in AFI

may be shared consistent with the Privacy Act, including in accordance with the routine uses, and applicable laws as described below including sharing with other DHS components and appropriate federal, state, local, tribal, territorial, foreign, multilateral, or international government agencies. This sharing will only take place after DHS determines that the receiving component or agency has a need to know the information and the information will be used consistent with the Privacy Act, including the routine uses set forth in this SORN, in order to carry out national security, law enforcement, customs, immigration, intelligence, or other authorized functions.

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

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which the U.S. Government collects, maintains, uses, and disseminates 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 for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. As a matter of policy (*Privacy Policy Guidance Memorandum 2007-1*, most recently updated January 7, 2009), DHS extends administrative Privacy Act protections to all persons, regardless of citizenship, where a

system of records maintains information on U.S. citizens and lawful permanent residents, as well as visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR Part 5.

Below is the description of the DHS/CBP—017 Analytical Framework for Intelligence (AFI) 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)/CBP—017 Analytical Framework for Intelligence (AFI)

System name:

U.S. Customs and Border Protection (CBP) Analytical Framework for Intelligence (AFI)

Security classification:

Unclassified, Sensitive, Classified.

System location:

Records are maintained within the Information Technology system called the Analytical Framework for Intelligence (AFI) at the CBP Headquarters in Washington, D.C., field offices, and in locations overseas where users are stationed.

Categories of individuals covered by the system:

1. Persons who are the subject of, related to, or associated with the subject of a finished intelligence product.

2. Persons whose information is responsive to a request for information (RFI).
3. Persons whose information is maintained in CBP systems described under the "Record Source Categories" below that are being indexed by AFI, such as:
    A. Persons, including operators, crew and passengers, who seek to, or do in fact, enter, exit, or transit through the United States or through other locations where CBP maintains an enforcement or operational presence.
    B. Crew members traveling on commercial aircraft that fly over the United States.
    C. Persons who are employed in or who engage in any form of trade, the transit of goods intended to cross the United States border, or other commercial transaction related to the importation or exportation of merchandise.
    D. Persons who serve as booking agents, brokers, or other persons who provide information on behalf of persons seeking to enter, exit, or transit through the United States, or to enter, exit or transit goods through the United States.
    E. Owners of vehicles that cross the border.
    F. Persons whose data was received by the Department as the result of a memorandum of understanding or other information sharing agreement or arrangement because the information is relevant to the

border security mission of the Department.

G. Persons who were identified in a narrative report, prepared by an officer or agent, as being related to or associated with other persons who are alleged to be involved in, who are suspected of, or who have been arrested for violations of the laws enforced or administered by DHS.

H. Persons who are alleged to be involved in, who are suspected of, who have been arrested for, or who are victims of violations of the laws enforced or administered by DHS.

I. Persons with outstanding wants and warrants.

J. Persons associated with matches to threshold targeting rules.

K. Persons who may pose a national security, border security, or criminal threat to the United States.

L. Persons who seek to board an aircraft to travel internationally who have been identified by the Centers for Disease Control and Prevention (CDC), U.S. Health and Human Services, as "No Boards" because of a highly contagious communicable disease.

M. Persons traveling across U.S. borders or through other locations where CBP maintains an enforcement or operational presence and who have a nexus to a law enforcement action.

Categories of records in the system:

AFI uses information from a variety of federal and commercial systems. If additional data is ingested and that additional data does not require amendment

of the categories of records in this SORN, the PIA for AFI will be updated to reflect that information. The updated PIA can be found at www.dhs.gov/privacy. Information from such source systems is incorporated into AFI's five general categories of records:

(1) *Finished intelligence products*: Intelligence products refer to tactical, operational, and strategic law enforcement intelligence products (hereinafter referred to as intelligence products). They include intelligence products that analysts have created based on their research and analysis of the source data contained in AFI and published in the system to make available as appropriate throughout CBP and DHS.

(2) *Requests for information (RFIs) and tasks and responses*: This includes requests for information or tasks (generic requests for work to be performed) that have been submitted through AFI. AFI will also store the responses to RFIs and those responses will fall in the same category of records as the RFIs unless the AFI analyst determines that a response should be converted to a finished intelligence product and makes it available more broadly.

(3) *Projects*: This includes projects created in AFI where an analyst can store source data for visualization and analysis and also share that information with other designated users. Projects may also contain analyst-compiled data from the source data described below and unfinished intelligence products that have not yet been published.

(4) *Index data*: AFI ingests subsets or portions of data from the CBP and

DHS systems described in "Record Source Categories" and creates an index of the searchable data elements, as described below in "source data." This index will indicate which source system records match the search term used, when a response to a query is compiled.

(5) *Source data*: AFI uses various types of data from CBP systems and other DHS systems as described in the individual system of records notices noted in "Record Source Categories" below. AFI also uses data from other federal agency systems and commercial data providers as noted in "Record Source Categories." Data elements may include but are not limited to:

a. Name
b. Alias
c. Addresses
d. Telephone and fax numbers
e. Tax ID number (*e.g.*, Employer Identification Number (EIN) or Social Security Number (SSN), where available)
f. Seizure number
g. Date and place of birth
h. Gender
i. Nationality
j. Citizenship
k. Physical characteristics, including biometrics where available (*e.g.*, height, weight, race, eye and hair color, scars, tattoos,

marks, fingerprints)

l. Familial relationships and other contact information

m. Occupation and employment information

n. Information from documents used to verify the identity of individuals (*e.g.*, driver's license, passport, visa, alien registration, citizenship card, border crossing card, birth certificate, certificate of naturalization, re-entry permit, military card, trusted traveler cards) including the:

    i. Type;

    ii. Number;

    iii. Date of issuance; and

    iv. Place of issuance.

o. Travel information pertaining to individuals, including:

    i. Information derived from an Electronic System for Travel Authorization (ESTA) application (where applicable) or I-94 arrival/departure information, where applicable;

    ii. Travel itinerary (*e.g.*, Passenger Name Record (PNR)); Advance Passenger Information System (APIS) information; and land border records including information submitted in advance of arrival or departure);

    iii. Date of arrival or departure, and means of conveyance

with associated identification (*e.g.*, Vehicle Identification Number, year, make, model, registration);

iv. Payment information;

v. Any admissibility determination; and

vi. Law enforcement data associated with an individual which is created by CBP or other government agencies.

p. Information pertaining to the importation and exportation of cargo and/or property, including but not limited to bills of lading, manifests, commodity type, and inspection and examination results

q. Identity and geospatial information obtained from commercial systems used to cross reference information contained in CBP systems

Authority for maintenance of the system:

Title II of the Homeland Security Act of 2002 (Pub. L. 107-296), as amended by the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108-458, 118 Stat. 3638); The Tariff Act of 1930, as amended; The Immigration and Nationality Act ("INA"), 8 U.S.C. §§1101, *et seq*.; the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L.110-53); the Antiterrorism and Effective Death Penalty Act of 1996 (Pub. L. 104-132, 110 Stat. 1214); SAFE Port Act of 2006 (Pub. L. 109-347); Aviation and Transportation Security Act of 2001 (Pub. L. 107-71); 6 U.S.C. § 202.

Purpose(s):

The purpose of this system is to enhance DHS's ability to: identify, apprehend, and/or prosecute individuals who pose a potential law enforcement or security risk; aid in the enforcement of the customs and immigration laws, and other laws enforced by DHS at the border; and enhance United States security.

AFI uses data to:

(1) identify individuals, associations, or relationships that may pose a potential law enforcement or security risk, target cargo that may present a threat, and assist intelligence product users in the field in preventing the illegal entry of people and goods, or identifying other violations of law;

(2) allow analysts to conduct additional research on persons and/or cargo to understand whether there are patterns or trends that could identify potential law enforcement or security risks; and

(3) allow finished intelligence product users with a need to know to query or receive relevant finished intelligence products.

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

Source data are to be handled consistent with the published system of records notice as noted in "Source Category Records." Source data that is not part of or incorporated into a finished intelligence product, a response to an RFI, project, or the index shall not be disclosed out of AFI. The routine uses below apply only to finished intelligence products, responses to RFIs, projects, and responsive compilations of the index and only as explicitly stated in each routine use. In addition to those disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, all or a portion of the

AFI records 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 U.S. Attorney Offices, or other federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is 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 of DHS in his/her official capacity;

3. any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or

4. the U.S. or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records.

This routine use applies to finished intelligence products, responses to RFIs, projects, and responsive compilations of the index.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains. This routine use applies to finished intelligence products, responses to RFIs, projects, and responsive compilations of the index.

C. To the National Archives and Records Administration (NARA) or other federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906 and for records that NARA

maintains as permanent records. This routine use applies to finished intelligence products, responses to RFIs, projects, and responsive compilations of the index.

D. To an agency, organization, or individual 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. This routine use applies to finished intelligence products, responses to RFIs, projects, and responsive compilations of the index.

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 harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) or harm to the individuals 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' efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

This routine use applies to finished intelligence products, responses to RFIs, projects, and responsive compilations of the index.

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 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. This routine use applies to finished intelligence products, responses to RFIs, projects, and responsive compilations of the index.

G. To the federal, state, local, tribal, or foreign government agencies or multilateral governmental organizations that submit an RFI, in order to identify individuals who present a risk to national security or to identify, apprehend, and/or prosecute individuals who are suspected of violating a law, where DHS has information responsive to the RFI and has determined that it is appropriate to provide that information in response to the RFI. This routine use applies to all responses to RFIs.

H. 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, agreement, or treaty where DHS determines that the information would assist in the enforcement of civil or criminal laws. This routine use applies only to finished intelligence products.

I. 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). This routine use applies only to finished intelligence products, responses to RFIs, and responsive compilations of the index.

J. 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 or criminal discovery, litigation, or settlement negotiations, or in response to a subpoena from a court of competent jurisdiction. This routine use applies to all AFI records, which include finished intelligence products, responses to RFIs, projects, and responsive compilations of the index.

K. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation. This routine use applies only to finished intelligence products.

L. To a federal, state, local, tribal, or foreign governmental agency or multilateral governmental organization for the purpose of consulting with that agency or entity: 1) to assist in making a determination regarding redress for an individual in connection with the operations of a DHS component or program; 2) for the purpose of verifying the identity of an individual seeking redress in connection with the operations of a DHS component or program; or 3) for the purpose of verifying the accuracy of information submitted by an individual who has requested such redress on behalf of another individual. This routine use applies only to finished intelligence products and responses to RFIs.

M. 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 for which the information may be relevant in countering the threat or potential threat. This routine use applies only to finished intelligence products.

N. 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. This routine use applies only to finished intelligence products.

O. To an organization or individual in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, or where the information is relevant and necessary to the protection of life or property. This routine use applies only to finished intelligence products.

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. This routine use applies only to finished intelligence products.

Q. 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. This routine use applies only to finished intelligence products.

Disclosure to consumer reporting agencies:

None.

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

Storage:

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

Retrievability:

Records may be retrieved by any search term, including name, personal identifier, date, subject matter or other criteria.

Safeguards:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Two principal types of users will access AFI: DHS analysts and DHS finished intelligence product users. DHS Analysts will use the system to obtain a more comprehensive view of data available to CBP, and then analyze and interpret that data using the visualization and collaboration tools accessible in AFI. Finished intelligence product users are officers, agents, and employees of DHS who have been determined to have a need to know based on their job description and duties. Finished intelligence product users will have more limited access to AFI, will not have access to the research

space or tools, and will only view finished tactical, operational, and strategic intelligence products that analysts published in AFI. Finished intelligence product users are not able to query the data from the source systems through AFI. If a finished intelligence product user requires the source data in order to take action or make a determination, he will be required to go to the source data to ensure that he is receiving the most accurate data available.

Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to AFI is limited 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:

Source data contained in AFI that has not been incorporated into a finished intelligence product, response to an RFI, or project will follow the retention schedule set forth in the applicable source data system of records notice, as noted in "Record Source Categories" below.

AFI projects that do not contain PII are retained for 30 years and are then deleted. Projects containing PII must be recertified annually for up to 30 years or the entire record is purged from the system. Requests for information (RFIs) and responses to RFIs, excluding finished intelligence products, are retained for 10 years and are then deleted. Finished intelligence products are retained in accordance with the NARA-approved record retention schedule by first maintaining the products as active in the system for a period of 20 years, and then transferring the records to the National Archives for permanent storage and retention. The index is maintained within AFI as a permanent

feature. Any changes to source system records, or the addition or deletion of source system records, will be reflected in corresponding amendments to the AFI index as the index is routinely updated. Legacy indices that are part of a project, responses to RFI, or finished intelligence product are maintained as part of those records.

System Manager and address:

Director of Advanced Analytics & Intelligence Systems, Office of Intelligence and Investigative Liaison, U.S. Customs and Border Protection, Ronald Reagan Building and Director, Targeting and Analysis, Systems Program Office, Office of Information and Technology, U.S. Customs and Border Protection.

Notification procedure:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records. To the extent that a record is exempted in a source system, the exemption will continue to apply. However, CBP will consider individual requests to determine whether or not information may be released. After conferring with the appropriate component or agency, as applicable, DHS may waive applicable exemptions in appropriate circumstances and where it would not appear to interfere with or adversely affect the law enforcement purposes of the systems from which the information is recompiled or in which it is contained. Additionally, CBP and DHS are not exempting any records that were ingested or indexed by AFI where the source system of records already provides access and/or amendment under the Privacy Act. 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 CBP's FOIA 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, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0655, Washington, D.C. 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or 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, you may obtain forms for this purpose from the Director, Disclosure and FOIA Operations, http://www.dhs.gov or 1-703-235-0790. In addition you must:

- Provide an explanation of why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created;
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

- If your request is seeking records pertaining to another living individual, include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) may not be able to conduct an effective search, and your 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:

AFI receives records and incorporates portions of records into an index of those records. Records are incorporated from the following CBP and DHS systems:

- ATS (last SORN published at 72 Fed. Reg. 43650 (August 6, 2007));
- APIS (last SORN published at 73 Fed. Reg. 68435 (November 18, 2008));
- ESTA (last SORN published at 76 FR 67751 (November 2, 2011));
- Border Crossing Information (BCI) (last SORN published at 73 Fed. Reg. 43457 (July 25, 2008));
- TECS (last SORN published at 73 Fed. Reg. 77778 (December 19, 2008));
- Nonimmigrant Information System (NIIS) (last SORN published at 73 Fed. Reg. 77739 (December 19, 2008));
- Seized Asset Case Tracking System (SEACATS) (last SORN published at 73 Fed. Reg. 77764 (December 19, 2008));

- Department of Homeland Security/All-030 Use of the Terrorist Screening Database System of Records (last SORN published at 76 FR 39408 (July 6, 2011));
- Enterprise Management Information System – Enterprise Data Warehouse (EMIS-EDW), including:
    a. Arrival and Departure Form (I-94) information from the Nonimmigrant Information System (NIIS) (last SORN published at 73 Fed. Reg. 77739 (December 19, 2008));
    b. Currency or Monetary Instruments Report (CMIR) obtained from TECS (last SORN for TECS published at 73 Fed. Reg. 77778 (December 19, 2008));
    c. Apprehension information and National Security Entry-Exit Program (NSEERS) information from ENFORCE (last SORN published at 75 Fed. Reg. 23274 (May 3, 2010));
    d. Seizure information from SEACATS (last SORN published at 73 Fed Reg. 77764 (December 19, 2008));
    e. Student and Exchange Visitor Information System (SEVIS) information (last SORN published at 75 Fed. Reg. 412 (January 5, 2010)); and

AFI accesses records from the following agencies, but the records are not part of the index:

- Department of State;
- Department of Justice/FBI;
- Department of Treasury; and

- Commercial information from commercial data providers and geospatial data providers.

Additionally, AFI permits analysts to upload and store any information from any source including public and commercial sources, which may be relevant to projects, responses to RFIs, or final intelligence products. Accepted requests for information may come from within or outside DHS where CBP determines it has responsive information and it is consistent with the purposes of this system.

Exemptions claimed for the system:

For index data and source data, as described under Categories of Records, to the extent that a record is exempted in a source system, the exemption will continue to apply. To the extent there is no exemption for giving access to a record under the source system, CBP will provide access to the information maintained in AFI.

Finished intelligence products, RFIs, tasks, and responses, and projects, as described under Categories of Records, pursuant to 5 U.S.C. § 552a(j)(2) of the Privacy Act, are exempt from the following provisions of the Privacy Act: 5 U.S.C. §§ 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f); and (g).

Finished intelligence products, RFIs, tasks, and responses, and projects, as described under Categories of Records, pursuant to 5 U.S.C. § 552a (k)(1) and (2), are exempt from the following provisions of the Privacy Act: 5 U.S.C. § 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

Dated: June 4, 2012

Mary Ellen Callahan

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2012-13813 Filed 06/06/2012 at 8:45 am; Publication Date: 06/07/2012]