Privacy Impact Assessment
for the

Analytical Framework for Intelligence (AFI)

June 1, 2012

Contact Point
Jim Gleason

Office of Intelligence and Investigative Liaison
U.S. Customs and Border Protection
(202) 344-1150

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

This Privacy Impact Assessment (PIA) covers the U.S. Customs and Border Protection's (CBP's) Analytical Framework for Intelligence (AFI) system. AFI enhances DHS's ability to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and 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 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 in the published Privacy Act System of Records Notice (SORN).

In order to mitigate privacy and security risks associated with the deployment of AFI, CBP has built technical safeguards into AFI and developed a governance process that includes the operational components of CBP, the oversight functions of the CBP Privacy Officer and Office of Chief Counsel, and the Office of Information and Technology. Additionally, the DHS Privacy Office provides oversight for the program.

This PIA is necessary because AFI accesses and stores personally identifiable information (PII) retrieved from DHS, other federal agency, and commercially available databases.

Overview

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) developed AFI to enhance DHS' ability to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and to improve border security. As part of CBP's authority to protect the border and enforce applicable laws at the border, CBP conducts research and analysis on its existing data systems to identify potential law enforcement or security risks and develops finished intelligence products for use. Currently, DHS analysts must employ dozens of searches/queries on individual data sources, and then manually read each search result for key elements such as names, dates, description of event, associates, and accomplices in a time-consuming process when conducting research and analysis. DHS analysts do not have a single access point to identify relevant data and use various tools to assist in the analysis of that data and develop intelligence products. The current process for handling Requests for Information (RFIs) also is not streamlined to ensure efficient responses.

AFI augments DHS' ability to gather and develop information about persons, events and cargo of interest by creating an index of the relevant data in the existing operational systems and providing DHS AFI analysts with different tools that assist in identifying non-obvious relationships. AFI allows analysts to generate tactical, operational, and strategic law enforcement intelligence products (hereinafter referred

to as "finished intelligence products"). Finished intelligence products better inform finished intelligence product users about why an individual or cargo may be of greater security interest based on the targeting and derogatory information identified in or through CBP's existing data systems. CBP currently utilizes transaction-based systems such as CBP TECS[1] (not an acronym) and the Automated Targeting System (ATS)[2] for targeting and inspections. AFI will enhance the information from those systems by utilizing different analytical capabilities and tools that provide link analysis between data elements as well as the ability to detect trends, patterns, and emerging threats.

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. DHS AFI analysts use AFI to conduct research on individuals and/or cargo/conveyances to understand whether there are patterns that could assist in the identification of potential law enforcement or security risks.

System Functions

AFI has four main components:

1. Analytic Capabilities

AFI provides a set of analytic tools to assist DHS AFI analysts (and thereby assist finished intelligence product users) to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and aids in the enforcement of customs and immigration laws and other laws enforced by DHS at the border. These tools include advanced search capabilities into existing DHS sources, and federated queries to other federal agency sources and commercial data aggregators to allow analysts to search several databases simultaneously. AFI tools will scan the query results, associate and extract similar themes, and present the results to the DHS AFI analyst in a manner that allows for easy visualization and analysis.

A. Index

In order to enable faster return of search results, AFI creates an index of the relevant data in existing operational DHS source systems by ingesting this data from source data systems (see below). AFI maintains the index of the key data elements that are personally identifiable in source data systems; however, if a particular source data system is not available because of technical issues, the DHS AFI analyst will not be able to retrieve the entire record from the source data system. The indexing engines refresh data from the originating system routinely depending on the source data system. AFI adheres to the records retention policies of the source data systems along with their user access controls.

DHS AFI analysts are able to perform searches with more efficacy in AFI because the data has been indexed, which allows for a search across all identifiable information in a record. Within AFI, this is a quick search that shows where a particular individual or characteristic arises. With other systems, a

[1] PIA: DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing
SORN: DHS/CBP-011 U.S. Customs and Border Protection TECS published December 19, 2008
[2] PIA: DHS/CBP/PIA-006 Automated Targeting System
SORN: DHS/CBP-006 Automated Targeting System published August 6, 2007.

similar search for a particular individual requires several queries across multiple systems to retrieve a corresponding response.

Records are incorporated from other CBP and DHS systems, including:

- ATS (last SORN published at 77 FR 30297 (May 22, 2012));
- Advance Passenger Information System (APIS) (last SORN published at 73 FR 68435 (November 18, 2008));
- Electronic System for Travel Authorization (ESTA) (last SORN published at 76 FR 67751 (November 2, 2011));
- Border Crossing Information (BCI) (last SORN published at 73 FR 43457 (July 25, 2008));
- TECS (last SORN published at 73 FR 77778 (December 19, 2008));
- Nonimmigrant Information System (NIIS) (last SORN published at 73 FR 77739 (December 19, 2008));
- Seized Asset Case Tracking System (SEACATS) (last SORN published at 73 FR 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:
    - Arrival and Departure Form (I-94) information from the Nonimmigrant Information System (NIIS) (last SORN published at 73 FR 77739 (December 19, 2008));
    - Currency or Monetary Instruments Report (CMIR) obtained from TECS (last SORN published at 73 FR 77778 (December 19, 2008));
    - Apprehension information and National Security Entry-Exit Program (NSEERS) information from ENFORCE (last SORN published at 75 FR 23274 (May 3, 2010));
    - Seizure information from SEACATS (last SORN published at 73 FR 77764 (December 19, 2008)); and
    - Student and Exchange Visitor Information System (SEVIS) information (last SORN published at 75 FR 412 (January 5, 2010)).

Additionally, AFI permits DHS AFI analysts to upload and store information that may be relevant from other sources, such as the Internet or traditional news media, into projects, responses to RFIs, or final intelligence products. RFIs, the responses to RFIs, finished intelligence products, and unfinished projects will also be searched when AFI users conduct analysis.

B. Federated Query:

DHS AFI analysts are able to perform federated queries against external data sources, including the Department of State, the Department of Justice/Federal Bureau of Investigation (FBI), as well as commercial data aggregators. Commercial data aggregators include sources available by subscription only that connect directly to AFI, and do not include information publicly available on the Internet. AFI tracks where DHS AFI analysts search and routinely audits these records. AFI uses data that is available from commercial data aggregators to complement or clarify the data it has access to within DHS. This includes information on individuals as well as geospatial data.

C. Analytical Tools:

AFI provides a suite of tools that assist in detecting trends, patterns, and emerging threats, and in identifying non-obvious relationships using the information maintained in the index and made accessible through the federated query. AFI makes these analytical tools available to permit the AFI analyst to employ the following methods to create finished intelligence products:

- Statistical analysis – modeling and statistical tools that can help analysts discover patterns or generalizations in the data. This analysis can produce models that can be used to identify similar patterns in other data or common characteristics among seemingly disparate data.
- Geospatial analysis – visualization tools that can display a set of events or activities on a map showing streets, buildings, geopolitical borders, or terrain. This analysis can help produce intelligence about the location or type of location that is favorable for a particular activity.
- Link analysis – visualization tools that can help analysts discover patterns of associations among various entities. This can produce a social network representation of the data.
- Temporal analysis – visualization tools that can display events or activities in a timeline to help an analyst identify patterns or associations in the data. This can produce a time sequence of events that can be used to predict future activities or discover other similar types of activities.

2. Workspace for Projects.

AFI supports DHS AFI analysts in the integration, research, analysis, and visualization of a large amount of data from disparate data sources, as described above. AFI allows DHS AFI analysts to create a "project" within the AFI workspace to capture research and analysis as the product or response is defined. It also functions as a shared workspace by allowing DHS AFI analysts to increase collaboration.

DHS AFI analysts will use this workspace to create finished intelligence products, which may be made available through AFI to other DHS AFI analysts and DHS finished intelligence product users. Finished intelligence products may also be shared pursuant to Routine Uses in the published Privacy Act SORN, with other authorities who do not have direct access to AFI.

3. Workflow Tracking System.

AFI allows DHS AFI analysts to track projects throughout their lifecycle from inception to finished intelligence product, or from RFI to response.

A. Finished Intelligence Products

Once analysts have prepared a finished intelligence product, that product goes through the supervisory review process and is then published to AFI. Analysts must designate the appropriate product classification for each intelligence product prior to publication so that it may be made available appropriately. Analysts must also select product type, areas, and subjects that will serve as document tags prior to publishing a finished intelligence product. The document tags will be used to narrow down the search for a finished intelligence product and will also allow AFI to push notifications of new products tagged as matching a finished intelligence product user's preferred types, areas, or subjects to that finished intelligence product user's homepage. AFI will only make finished products available to those finished intelligence product users who have permission to view that type of information based on access allowed via the finished intelligence product user's profile.

B. RFI Request and Response

AFI provides a platform for staging RFIs and the responses to those requests. AFI will centrally maintain the requests, the research based on those requests, and any subsequent products responsive to those requests in one place and also make available that information as appropriate. When an RFI is made to CBP, CBP will review the RFI to determine whether it has the authority to respond to the RFI and whether it has responsive records. AFI will allow DHS AFI analysts to search the requests and the responses to determine if CBP has already received a particular or similar request. If, through the supervisory review process, CBP determines that a response to an RFI should be created into a finished intelligence product, the DHS AFI analyst will use the process described above to share the information more broadly.

4. Information Sharing Platform for Finished Intelligence Products

Finished intelligence products refer to tactical, operational, and strategic law enforcement intelligence products. They include intelligence products that DHS AFI 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.

Finished intelligence product users are officers, agents, and employees of DHS who have been determined to have a need to know 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, meaning they may view finished intelligence products that analysts published in AFI, but cannot access the research space or tools. Finished intelligence product users are not able to query the data from the source systems through AFI.

In order to mitigate the risk of certain sensitive categories of data being used for inappropriate purposes, AFI requires that analysts mark or tag intelligence products containing such data prior to publication to the system. The marking ensures that only those finished intelligence product users that have a need to know and who are authorized to view that type of data may access the product. By marking the product, an analyst creates restrictions with respect to the group of finished intelligence product users who may view the product. By requiring finished intelligence product users to identify, through supervisors, those markings relevant to their mission and role and only permitting access where a

finished intelligence product user tag and a product tag match, AFI creates a further means of safeguarding sensitive information.

AFI is used internally by DHS to share finished intelligence products. Finished intelligence products may be shared externally through regular law enforcement and intelligence channels to authorized users with a need to know, pursuant to routine uses in the published Privacy Act SORN for AFI.

Users and Uses

AFI will be used by OIIL analysts, Border Patrol agents, Air and Marine officers, Office of Field Operations (OFO) officers, and OITA specialists.

Based on job description and specific job duties, individuals will be assigned one of two principal user types: DHS analysts and DHS finished intelligence product users. Within these two principal user types there are a number of specific roles:

1. DHS AFI Analysts

DHS AFI 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. DHS AFI analysts will use the data in AFI to identify individuals, associations, relationships, or patterns that may pose a potential law enforcement or security risk, target cargo that may present a threat, and assist finished intelligence product users in the field in preventing the illegal entry of people and goods, or identifying other violations of law or regulations at and/or between ports of entry.

Only DHS AFI analysts will have access to the analytical tools. Typically, a DHS AFI analyst will maintain this data either in the analytical tool or in the AFI project space where collaboration with other designated users on the information may occur. A DHS AFI analyst may choose to archive this data upon completion of an intelligence product or simply maintain it as part of an AFI project for future evaluation and analysis. The data maintained in AFI are subject to an annual PII re-certification process, which requires that users recertify any user-provided information marked as containing PII to ensure its continued relevance and accuracy.

If a DHS AFI analyst finds actionable terrorism-related, law enforcement, or intelligence information, they may use this relevant information to produce a report, create an alert, or take some other appropriate action within DHS' mission and authorities. In addition to using AFI as a workspace to analyze and interpret data, DHS AFI analysts may submit RFIs, assign tasks, or create intelligence products based on their research or in response to an RFI.

2. Finished Intelligence Product Users

Finished intelligence product users will have more limited access to AFI and will only view finished tactical, operational, and strategic intelligence products that DHS AFI analysts publish in AFI. When a finished intelligence product user accesses AFI, they may either conduct a search to view finished products or select their preferences within the system so that certain finished products are automatically pushed to their homepage. For example, if a finished intelligence product user wishes to view all products related to narcotics, they may select that category in their preferences and all products tagged as

pertaining to narcotics will cause a notification to be pushed to that user. If a finished intelligence product user does not select any preferences, they will only be able to view finished products by conducting a search. Access to products will be limited based on the finished intelligence product user's level of clearance and system user rights and privileges.

When a user sets their preferences within the system, products tagged as matching their preferred types, areas, or subjects will be pushed to that user's homepage. When a user conducts a search for products, AFI will only display those results a user has permission to view based on the designated product classification. Finished intelligence product users will not have access to the research space and will only view published finished intelligence products.

Privacy Risks and Mitigations

While AFI will increase the efficient and effective use of information at CBP, it also creates new privacy risks, which are mitigated by technical solutions, governance, clearly established procedures, and trained staff.

AFI indexes information from many different source data systems and allows for a more efficient search of that data as compiled in a manner that was not previously accessible in one system. This is beneficial because it allows DHS AFI analysts to perform link analysis to discover patterns or associations among various entities. Several privacy risks, however, arise from the compilation of data collected from multiple source data systems. AFI has employed a variety of solutions to mitigate these risks.

A risk in maintaining an index of data from several different systems in one database is that AFI may provide users with greater access to data than their individual system rights permit. To combat this risk, the source system that performed the original collection of data maintains control of that data even though the data is co-located in both the source system and in AFI. Accordingly, only DHS AFI analysts authorized to access the data in the source system have access to that same data through AFI. This is accomplished by passing individual user credentials from the originating system or through a previously approved certification process in another system.

Finished intelligence product users and DHS AFI analysts have access to finished intelligence products. Only DHS AFI analysts have access to the source data, projects, and analytical tools maintained in AFI.

Another privacy risk is that AFI may retain incorrect information because it draws upon other systems to collect information instead of collecting information directly from the original source. In order to mitigate the risk of AFI retaining incorrect, inaccurate, or untimely information, AFI routinely updates its index to ensure that only the most current data are available to its users. Any changes to source system records, or the addition or deletion of a source system record, will be reflected in the corresponding amendments to the AFI index when the index is updated. Further, when a user accesses individual records, the records are retrieved directly from the source system to ensure data quality. AFI also requires that users recertify annually any user-provided information marked as containing PII to ensure its continued relevance and accuracy. If the information is not recertified, it is automatically purged from the system.

In order to combat the risk of authorized users conducting searches for inappropriate purposes, AFI performs extensive auditing that records the search activities of all users. AFI has built-in system controls that identify what particular users are able to view, query, and/or write as well as audit functions that are routinely reviewed.

Finally, the risk in AFI compiling data that was originally collected by several other systems is that the data may not be used consistent with the purpose for which it was originally collected. To prevent this misuse, CBP has created a governance board, described below, to oversee the development and use of AFI.

AFI is being designed and developed in an iterative, incremental fashion. As AFI evolves to include new classes of data and new functionality, this PIA will be updated. In order to ensure that the system is built and used consistent with the authorities of the Department, CBP has created a governance body, made up of individuals from OIIL, OFO, CBP Privacy Office, Office of Chief Counsel and OIT who review the requested changes to the system on a quarterly basis and determine whether additional input is required. The governance board will direct the development of new aspects of AFI, which will include reviewing and approving new or changed uses of AFI, new or updated user types, and new or expanded data to be made available in or through AFI. The DHS Privacy Office will conduct a privacy compliance review within 12 months of the system's operational deployment.

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?

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.

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

The information contained in the source systems performing the original collection is covered by the individual SORNs for those systems as listed in Appendix B. AFI is also publishing its own SORN to cover the RFIs, tasks, responses to RFIs, finished intelligence products, the index, and DHS AFI analyst-created projects.

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

The Certification & Accreditation (C&A) of AFI is pending approval of this PIA. The government systems accessed or used by AFI have undergone C&A and are covered by their respective Authorities to Operate (ATOs).

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

AFI is in the process of completing NARA requirements for data retention to obtain a records schedule. AFI is proposing that its retention is the same as the retention schedule presently in place for similar records within the Department. As such, projects will be retained for up to 30 years, RFIs and responses to RFIs will be retained for 10 years, and finished intelligence products will be retained for 20 years.

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 information contained in AFI is not covered by the Paperwork Reduction Act because the system does not collect information directly from the public.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

The AFI system does not collect information directly from the public. Rather, AFI performs searches for and accesses information collected and maintained in other systems, including information from both government owned sources and commercial data aggregators. Additionally, DHS AFI analysts may upload information that the user believes is relevant to a project, including information publicly available on the Internet. There are six categories of data containing PII that AFI uses, disseminates, or maintains. The types of data elements that may be maintained in the six categories includes, but is not limited to: full name, date of birth, gender, travel information, passport information, country of birth, physical characteristics, familial and other contact information, importation/exportation information, and enforcement records. See Appendix A for a more comprehensive list of PII data stored in AFI.

1) *DHS-Owned Data*: AFI automatically collects and stores selected data from DHS systems. AFI receives records from ATS (including: APIS, Electronic System for Travel Authorization (ESTA), TECS Incident Report Logs and Search, Arrest, Seizure Reports (S/A/S), Primary Name Query, Primary Vehicle Query, Secondary Referrals, TECS Intel Documents, and VISA Data),

EMIS-EDW (including: Arrival and Departure Form (I-94), Currency or Monetary Instruments Report (CMIR), ENFORCE apprehension, inadmissible and seizure information, National Security Entry-Exit Program (NSEERS) information from ENFORCE, Student and Exchange Visitor Information System (SEVIS) information), and case information from the Targeting Framework. This data is indexed so that the system may retrieve it by any identifier maintained in the record. As information is retrieved from multiple sources it may be joined to create a more complete representation of an event or concept. For example, a complex event such as a seizure that is represented by multiple records may be composed into a single object, for display, representing that event.

2) *Other Government Agency Data*: AFI obtains imagery data from the National Geospatial-Intelligence Agency and obtains other government agency data to the extent available through ATS, such as identity and biographical information, wants and warrants, Department of Motor Vehicle (DMV) data, and data from the Terrorist Screening Database. A fuller discussion of the other government agency data which may be accessed through ATS can be found in the ATS PIA.

3) *Commercial Data*: AFI collects identity and imagery data from several commercial data aggregators so that DHS AFI analysts can cross-reference that information with the information contained in DHS-owned systems. Commercial data aggregators include sources available by subscription only that connect directly to AFI.

4) *DHS AFI Analyst-Provided Information*: This includes any information uploaded by an authorized user either as original content or from an *ad hoc* data source, such as the Internet or traditional news media. DHS AFI analyst-provided information may include textual data (such as official reports a user has seen as part of their duties or segments from a news article), video and audio clips, pictures, or any other information the user believes is relevant. User-submitted RFIs and projects are also stored within AFI, as well as the responses to those requests.

5) *DHS AFI Analyst-Created Information:* AFI maintains user-created projects as well as finished intelligence products. Finished intelligence products are made available through AFI to finished intelligence users.

6) *Index Information*: AFI ingests subsets of data from the CBP and DHS systems to create an index of the searchable data elements. The index will indicate which source system records match the search term used.

DHS data sources utilized in AFI covered by this PIA are unclassified.

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

AFI does not collect information directly from individuals, but rather accesses information collected, generated, and stored by and in other systems. The DHS-owned data in AFI comes from the ATS, APIS, BCI, ESTA, NIIS, TECS, SEACATS, and EMIS-EDW, which includes arrival and departure

information, CMIR, ICE's EID, and SEVIS information. See Appendix B for listing of the relevant SORNs.

Other government agency data is obtained from the Department of State Consular Consolidated Database (CCD),[3] the National Crime Information Center (NCIC), the National Law Enforcement Telecommunications System (Nlets), and the Federal Bureau of Investigation Terrorist Screening Center's Terrorist Screening Database Watchlist Service (TSDB-WLS)[4] through ATS. Additionally, AFI collects data from the National Geospatial-Intelligence Agency. Commercial data is obtained from different commercial data aggregators for both PII as well as geospatial data.

All other information is collected directly from DHS AFI analysts. DHS AFI analysts will provide information that comes from their knowledge or any other data source, such as reference materials or open source data that is uploaded into AFI on an *ad hoc* basis. DHS AFI Analysts will create projects, responses to RFIs, and finished intelligence products within AFI. Index data is generated by processing stored DHS data, DHS AFI analyst-provided data, projects, responses to RFIs, and finished intelligence products through search engines.

All DHS AFI analysts have access to the Internet and may upload information available through an Internet search into a project.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

AFI uses data from commercial data aggregators and publicly available information to complement or clarify the data it has access to within DHS. AFI collects additional identity information, watch list data, and geospatial data from commercial data aggregators.

This data is used to cross-check, confirm, and broaden the scope of information available within AFI about an individual of interest. The geospatial data is also used to support visualization of the data on maps. Specific query results may be saved within the AFI system by the users if the results are deemed valuable for ongoing analysis or incorporation into finished intelligence products.

As stated above, all DHS AFI analysts have access to publicly available information on the Internet and may upload this information into a project via the DHS High Assurance Gateway (HAG).

2.4 Discuss how accuracy of the data is ensured.

Because AFI does not collect information directly from the public or any other primary source, it depends on the system(s) performing the original collection. DHS AFI analysts will use a variety of data sources available through the source systems to verify and correlate the available information to the greatest extent possible.

[3] PIA available at http://www.state.gov/documents/organization/93772.pdf.
[4] TSDB: SORN published at 76 FR 39408 (July 6, 2011).

The accuracy of DHS-owned data, other federal agency data, and data provided by commercial data aggregators is dependent on the original source. DHS AFI analysts are required by policy to make changes to the data records in the underlying DHS system of record if they identify inaccurate data and alert the source agency of the inaccuracy. AFI will then reflect the corrected information. Additionally, as the source systems for other federal agency data or commercial data aggregators correct information, queries of those systems will reflect the corrected information.

DHS AFI analysts are required to vet data in accordance with standard operating procedures and training manuals to ensure that the data used is accurate. DHS AFI analyst-provided information is stored in a collaborative workspace where other analysts can review and challenge it. Finished intelligence products, responses to RFIs, and project contents are subject to peer and supervisor review to ensure accuracy before publication. Index data is updated routinely, and DHS AFI analyst-provided products, responses to RFIs, and project information is updated every few minutes to ensure that it is as complete and accurate as possible.

If erroneous information is published in a finished intelligence product, a revised product is published to correct the information or note the questionable fact or content, and the incorrect product is removed from the repository. For any products that were externally disseminated and need recall or correction, a recall message or revised product will be disseminated to the recipients of the original product(s) with appropriate instructions.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

In addition to the risks accumulated by the underlying systems which AFI accesses (such as ATS, CCD, and others), the following potential risks related to AFI's collection of data have been identified:

Privacy Risk:

Because AFI permits DHS AFI analysts to provide their own analysis and incorporate data from commercial data aggregators and publicly available sources rather than using only directly collected information, it is possible for a DHS AFI analyst, commercial data aggregator, or public source to, accidentally or purposefully, provide incorrect or biased information.

Mitigation:

AFI requires that all DHS AFI analyst-provided information be fully attributable to the analyst who provided it. The auditing and peer review functions further serve to ensure that DHS AFI analyst-provided information is reviewed for flaws. If a DHS AFI analyst provides incorrect or biased information, the information can be corrected and the DHS AFI analyst can be disciplined, if appropriate.

Data from commercial data aggregators and publicly available sources is vetted by DHS AFI analysts for accuracy by cross checking the information against multiple sources. Information in intelligence products from commercial data aggregators and publicly available sources is checked for accuracy using the same review process as other information in AFI.

Privacy Risk:

Because AFI draws upon DHS-owned, other federal agency, and commercial data aggregators to obtain data instead of collecting directly from individuals, there is a risk that the data in AFI will become outdated.

Mitigation:

AFI's index routinely refreshes from its various source systems, so that it accurately reflects any changes to the records contained in the underlying source systems and the addition or deletion of those records. When a DHS AFI analyst accesses a record through AFI, the record is retrieved from the underlying source system to ensure that only the most current data is available to DHS AFI analysts. Additionally, when a DHS AFI analyst conducts a query, any changes, additions, or deletions of records from commercial data aggregators will be reflected in that query.

Privacy Risk:

AFI receives data from multiple border security and compliance systems that while determined to be compatible with the AFI mission still present a risk given the varied contexts in which the underlying information was collected and the potential for the information to be taken out of context. Further there is risk of mission creep in that additional data sources will be added that are not compatible with the purpose or mission of AFI.

Mitigation:

AFI accesses information from border security and compliance systems that share purposes compatible with its mission. Routine audits of system access serve to ensure that analysts employ information consistent with the purposes for which it was collected. The governance body for AFI ensures that the system architecture does not create access or linkages to other systems with incompatible purposes for the law enforcement, border security, and counter-terrorism missions of AFI. In addition to these protections, the DHS Privacy Office will conduct a privacy compliance review within 12 months of the system's operational deployment.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

CBP is collecting the information contained within AFI to allow DHS AFI analysts to generate intelligence products that better inform officers, agents, and employees in the field about the context pertaining to the targeting and derogatory information identified in underlying source systems and to enhance how CBP uses data it already collects by utilizing analysis tools that detect trends, patterns, and emerging threats.

DHS AFI analysts will use AFI 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. DHS AFI analysts will use the data in AFI to identify individuals, associations, relationships, or patterns that may pose a potential law enforcement or security risk, target cargo that may present a threat, and assist finished intelligence product users in the field in preventing the illegal entry of people or goods, or identifying other violations of law or regulations at and/or between ports of entry. When a DHS AFI analyst conducts a search, AFI will perform the query on the index as well as across multiple systems from the other Federal agency systems, and commercial systems listed in section 2.2. Indexed data facilitates efficient searching of large databases for terms that occur in fielded or free-text data. Only DHS AFI analysts authorized to access the data in the underlying system have access to that same data through AFI. In allowing DHS AFI analysts to perform a single query across multiple systems, AFI reduces the time spent searching each individual system and reduces the load placed on those systems through repeated queries. DHS AFI analyst-provided information and data obtained from commercial sources is used to complement or clarify data from internal DHS sources, and imagery data allows analysts to view information in a geographic context.

DHS AFI analysts will use the analytical tools in AFI such as link analysis tools, temporal analysis tools, statistical analysis tools, and geospatial analysis tools to conduct analysis and create final reports. Typically, a DHS AFI analyst will maintain the raw data in either the analytical tool or in the AFI project space where collaboration with other designated AFI users on the information may occur. A DHS AFI analyst may choose to archive this data upon completion of an intelligence product or simply maintain it as part of an AFI project for future evaluation and analysis. If a DHS AFI analyst finds actionable terrorism-related, law enforcement, or intelligence information after conducting a search and performing analysis on the raw data, they may use relevant information to produce a report, create an alert, or take some other appropriate action within DHS' mission and authorities.

In addition to using AFI as a workspace to analyze and interpret data, AFI works as a workflow management tool allowing analysts to submit RFIs, supervisors to assign research, and supervisors to review and approve finished intelligence products or responses to RFIs. AFI maintains that research (and any intelligence products subsequently created from that research) in a single location, facilitates the sharing of finished intelligence products within DHS, and tracks sharing outside of DHS.

Finished intelligence product users are officers, agents, and employees of DHS who have been determined to have a need to know 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 and will only use the system to view finished tactical, operational, and strategic intelligence products that analysts published in AFI. When a finished intelligence product user accesses AFI, they may either conduct a search to view finished products or select their preferences within the system so that certain finished products are pushed to their homepage. Access to products will be limited based on the finished intelligence product user's level of clearance and system user rights and privileges.

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.

AFI creates and retains an index of searchable data elements in existing operational DHS source systems by ingesting this data through and from its source systems. The index will indicate which source system records match the search term used. AFI maintains the index of the key data elements that are personally identifiable in source data systems, but if a particular source data system is not available because of technical issues, the DHS AFI analyst will not be able to retrieve the entirety of the responsive record. The indexing engines refresh data from the originating system routinely. 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.

AFI also includes a suite of tools designed to give DHS AFI analysts visualization, modeling, collaboration, analysis, summarization, and reporting capabilities. These include cross-domain search, text analysis, link analysis (social network analysis), statistical analysis, and geospatial analysis.

Specific types of analysis include:

- Statistical analysis – modeling and statistical tools that can help analysts discover patterns or generalizations in the data. This analysis can produce models that can be used to identify similar patterns in other data or common characteristics among seemingly disparate data.
- Geospatial analysis – visualization tools that can display a set of events or activities on a map showing streets, buildings, geopolitical borders, or terrain. This analysis can help produce intelligence about the location or type of location that is favorable for a particular activity.
- Link analysis – visualization tools that can help analysts discover patterns of associations among various entities. This can produce a social network representation of the data.
- Temporal analysis – visualization tools that can display events or activities in a timeline to help an analyst identify patterns or associations in the data. This can produce a time sequence of events that can be used to predict future activities or discover other similar types of activities.

The results of this analysis are used to generate finished intelligence products, responses to RFIs, and projects. The finished intelligence products will be published in AFI for finished intelligence product users to search.

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

CBP is the only component with assigned roles and responsibilities within the system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk:

Authorized users of AFI could utilize their access for unapproved or inappropriate purposes, such as performing searches on themselves, friends, relatives, or neighbors.

Mitigation:

AFI performs auditing that records the search activities of all users. These audit logs are reviewed periodically and any inappropriate use will be referred to the appropriate internal investigators (such as Internal Affairs, the Joint Intake Center, or others as required) for handling. The detection of inappropriate use will also result in the suspension of the user's access to AFI until the use can be investigated. AFI's auditing capabilities are discussed in greater depth later in this document. This auditing capability ensures that information is handled correctly and in accordance with the uses described in this document and DHS/CBP policies and procedures.

It is the policy of the U.S. government that employees and contractors have no privacy expectations associated with the use of any DHS network, system, or application. This policy is in full effect for AFI. Audit trails are created throughout the process and are reviewed if a problem or concern arises regarding the use or misuse of the information. When a user goes through the log-in process, he must acknowledge the consent to monitoring or he cannot use the system.

AFI uses security and auditing tools to ensure that information is used in accordance with CBP policies and procedures. The security and auditing tools include:

- Role-Based Access Control (RBAC) determines a user's authorization to use different functions, capabilities, and classifications of data within AFI.
- Discretionary Access Control (DAC) determines a user's authorization to access individual groupings of User Provided data.
- Data are labeled and restricted based on data handling designations and need-to-know for SBU (FOUO, PII, SSI, LES).
- AFI is developed to Intelligence Community Protection Level 2+ (PL2+) standards to prevent unauthorized access to data, ensuring that isolation between users and data is maintained based on need-to-know.
- Application logging and auditing tools monitor data access and usage, as required by the information assurance policies against which AFI was designed, developed, and tested (including Director of Central Intelligence (DCID) 6/3 and DHS MD 4300 A/B).

Privacy Risk:

Because AFI compiles data from multiple systems, users will access information from several systems that previously were not accessible in one system. Some information compiled is not necessarily indicative of illegal activity and could be taken out of context.

Mitigation:

Information identified and accessed through AFI for the purpose of incorporation into an intelligence product or a response to an RFI will bear a rational relationship to the scope of the analysis contained in the product or response. The clearance process for publishing a product or disseminating a response back to a requestor involves supervisory review to ensure that the analysis and conclusions of the product or response are germane to the purpose for which the product or response was intended.

Privacy Risk:

AFI does not collect information directly from the public, so individuals may not have notice that their information is used by AFI.

Mitigation:

AFI is publishing a SORN and this PIA to inform individuals what information is contained within AFI and how it is used.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

AFI will be publishing a SORN to cover the RFIs, responses to RFIs, finished intelligence products, the index and analyst created projects, however, AFI does not collect any information directly from individuals, and therefore does not have an opportunity to provide notice of such collection. Notice of collection by the underlying government systems performing the original collection is described in the individual PIAs and SORNs for those systems. See Appendix B for listing of the relevant SORNs. Commercial data aggregators collect information from publicly available and proprietary records, and therefore do not likely provide notice to the individual prior to collection.

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

AFI does not collect information directly from individuals. As such, individuals do not have opportunities to decline to provide information, consent to uses, or opt out of projects. To the extent that it is practical, AFI relies on the systems from which it draws information to provide those opportunities to the individuals from which this information is collected. Additionally, as the government systems from which AFI draws information are law enforcement systems that collect information that individuals are required to provide by statutory mandate, these individuals do not have an opportunity to decline to provide the required information, opt out, or to consent to uses. Further, DHS/CBP does not have the ability to provide individuals with the opportunity to consent to uses or decline to provide information to commercial sources because it does not control those systems and cannot provide notice other than through this document.

4.3 Privacy Impact Analysis: Related to Notice

Each of the various systems that perform the original collection and from which AFI draws information are subject to their own notice requirements and mechanisms for such notification. AFI itself provides no such notice aside from its SORN and this PIA.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

The retention period for the information contained in AFI varies depending on the type of data. DHS owned data is retained in accordance with the SORN for the underlying system from which the data is obtained.[5] Once an underlying source system deletes or changes the data, AFI will delete or change its data during its next refresh from that system. DHS AFI analyst-created projects without PII are retained for 30 years and are then deleted. Projects containing PII must be recertified annually or the information is purged from the AFI system. RFIs and responses to RFIs, excluding finished intelligence products, are

[5] ATS: Last SORN published at 77 FR 30297 (May 22, 2012).
APIS: Last SORN published at 73 FR 68435 (November 18, 2008).
BCI: Last SORN published at 73 FR 43457 (July 25, 2008).
ENFORCE: Last SORN published at 75 FR 23274 (May 3, 2010).
ESTA: Last SORN published at 73 FR 32720 (June 10, 2008).
NIIS: Last SORN published at 73 FR 77739 (December 19, 2008).
SEACATS: Last SORN published at 73 FR 77764 (December 19, 2008).
SEVIS: Last SORN published at 75 FR 412 (January 5, 2010).
TECS: Last SORN published at 73 FR 77778 (December 19, 2008).

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.

5.2 Privacy Impact Analysis: Related to Retention

AFI's analytic use of the information gathered by existing systems coupled with its retention policies results in the following risks:

Privacy Risk:

Because AFI accesses and indexes information from other systems, it is possible that incorrect information could be indexed in AFI and then corrected in the underlying system. Consequently, a search in AFI could return the outdated information.

Mitigation:

AFI periodically refreshes the indices built from data residing in underlying systems to ensure that only the most current versions are available to users. Further, when a user accesses individual records matching a search (rather than simply the list of results), the records are retrieved directly from the underlying source system. This ensures that users see the most up-to-date information.

Privacy Risk:

Many analytic intelligence products are based on or contain so-called "perishable" information. Such products lose accuracy or relevance after a finite period of time, and therefore there is a risk that resulting agency actions involving with the potential to affect encountered persons will be handled inappropriately because the information is no longer accurate or relevant.

Mitigation:

DHS AFI analysts are required to update finished intelligence products and responses to RFI if they discover the information previously provided was inaccurate or incorrect. Additionally, AFI requires that DHS AFI analysts recertify, on an annual basis, any information marked as containing PII. This gives the user an opportunity to review all of the information, including the PII, and ensure its continued relevance and accuracy, and limits the time that "perishable" information remains in the system.

Privacy Risk:

As AFI provides access to and retains a wealth of information, it may become a target for unauthorized users (hackers).

Mitigation:

AFI employs both system level security and application level security, including role-based access control (RBAC) and discretionary access control (DAC), and has undergone a Certification and

Accreditation (C&A) process. Further, CBP conducts routine audits and system checks to ensure the relevance of controls and markings, and to protect the information over time.

Privacy Risk:

AFI may retain more information than is necessary for any specific request or research project.

Mitigation:

By indexing the data, AFI allows for a more effective and efficient query of the data, without retaining a complete copy of the responsive data. This reduces the number and volume of individual records that must be reviewed to identify the relevant record.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

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.

The information shared by AFI outside of DHS are the finished intelligence products, responses to RFIs where the response is determined to have relevance to more users than the requestor, and, in limited circumstances, responsive compilations of the index, which may contain PII. This information may be shared with any law enforcement, counterterrorism, or national security governmental organization, in a manner consistent with the relevant routine use identified in the AFI SORN.

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

The sharing of PII outside of the Department is compatible with the original collections listed in the SORNs of the source systems. Generally, information is shared for law enforcement, intelligence, and/or national security purposes and with contractors working for the federal government to accomplish agency functions related to the system of records.

6.3 Does the project place limitations on re-dissemination?

Users of AFI will utilize the processes and procedures already established within DHS and CBP with regard to dissemination of data and information. Users will follow the Third Agency Rule, which mandates that prior to sharing information or data to a third agency (not involved in the original sharing agreement), the agency that intends to share will acquire consent from the agency (most likely CBP or DHS) that provided the data or information. New agencies that are added as users within AFI will be notified of this mandate, and will be required to follow this process as a condition of becoming users within AFI. Only individuals with a need to know will be able to gain access to the finished intelligence products. Generally, non-CBP individuals will not have access to AFI's index or to the RFIs within AFI.

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

AFI utilizes the existing processes and procedures within DHS and CBP for recording disclosures of information as appropriate to the situation causing the disclosure, and does not establish or maintain an additional record of the disclosures within the AFI system. Policies and procedures in use include: DHS Directive 047-01 Privacy Policy and Compliance, DHS Instruction 047-01-001 Privacy Policy and Compliance, DHS form 191 Accounting for Disclosure, DHS Form 11000-8 Disclosure Record, DHS Form 11000-10 Document Record of Transmittal, DHS Form 11000-10 Record of Security Violation, CBP Form 12 Report of Congressional Contact, and CBP Form 236 Interagency Agreement.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk:

Authorized users are exposed to PII as a routine part of their official duties. These users may make inappropriate disclosure of this information, either intentionally or unintentionally.

Mitigation:

All AFI users are required to complete training on privacy, including the appropriate and inappropriate uses and disclosures of the information they receive as part of their official duties. A user's use of the system and access to data is monitored and audited. Should a user inappropriately disclose this information, they are subject to loss of access and the disclosure will be referred to the appropriate internal investigation entity. Additionally, users are required to undergo system access recertification annually.

Privacy Risk:

Finished products containing incorrect information may be disseminated.

Mitigation:

As with other intelligence systems, this risk is mitigated through policies describing the correction and re-dissemination process. All products that leave AFI are marked with their classification and originating ownership, as well as instructions which direct the reader to contact CBP OIIL before using or disseminating the information.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Because AFI contains sensitive information related to intelligence, counterterrorism, homeland security, and law enforcement programs, activities, and investigations, DHS has exempted AFI from the access and amendment provisions of the Privacy Act of 1974, pursuant to 5 U.S.C. §§ 552a(j)(2) and (k)(2).

For index data and source data, as described under Categories of Records in the published SORN, 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)(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)(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), and (f).

Notwithstanding the applicable exemptions, CBP reviews all such requests on a case-by-case basis. Where such a request is made, and access would not appear to interfere with or adversely affect the national or homeland security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of CBP, and in accordance with procedures and points of contact published in the applicable SORN. Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a Freedom of Information Act (FOIA) or Privacy Act request in writing to

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
Mint Annex Building
1300 Pennsylvania Avenue, NW
Washington, DC 20229

FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. Specific FOIA contact information can be found at http://www.dhs.gov/foia under *contacts*.

While DHS has exempted this system from the access and amendment provisions of the Privacy Act, individuals may make a request to view their records. If an individual requests information that may

be in AFI, a search will be conducted of the finished intelligence products, responses to RFIs, projects, and the index, including information contained in underlying source systems. When seeking records about oneself from this system of records or any other CBP system of records, the request must conform to the Privacy Act regulations set forth in 6 CFR Part 5. An individual must first verify their identity, meaning that they must provide full name, current address, and date and place of birth. The request must include a notarized signature or be submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, forms for this purpose may be obtained from the Director, Disclosure and FOIA, http://www.dhs.gov or 1-866-431-0486. In addition, the following should be provided:

- An explanation of why the individual believes the Department would have information on them,
- Details outlining when they believe the records would have been created,
- If the request is seeking records pertaining to another living individual, it must include a statement from that individual certifying his/her agreement for access to his/her records.

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

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

The data accessed by AFI from source systems may be corrected by means of the processes described in the PIAs for those systems. Since AFI draws upon other source systems for its data, 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 periodically updated.

DHS AFI analysts are responsible for the integrity of the data they provide. Should erroneous information be entered, the user is required to correct their entry immediately upon determining it to be incorrect. This requirement applies to any data a user has access to, not just data provided by the user.

At times, erroneous information may be published in a finished intelligence product. When incorrect information is discovered, a revised product will be published to correct the information or note the questionable fact or content, and the incorrect product will be removed from AFI. For any products that were externally disseminated and needing recall or correction, a recall message or revised product will be disseminated to the recipients of the original product(s) with appropriate instructions.

As noted in 7.1 above, any requests from the public for information in AFI will be reviewed on a case-by-case basis.

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

Individuals are notified of the procedures for correcting their information through the SORNs describing each of the underlying systems from which AFI accesses information, as well as the AFI SORN.

7.4 Privacy Impact Analysis: Related to Redress

Given the sensitive nature of AFI, a robust program to permit access, review, and correction of raw information and products (finished or in-progress) cannot be provided. This lack of direct access and a formal redress mechanism represent a risk to individual privacy, however it is necessary given the heightened sensitivity of and potential harm to government activities supported by AFI. While individuals will not have a formal mechanism for access or redress, CBP has internal mechanisms to correct inaccuracies and protect against abuse through the information system security protections and controls established within the AFI system.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

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

The AFI system implements extensive auditing through the various applications that comprise the system. Such logs are collected at three distinct levels: operating system, database, and application.

The application level, which is the level at which user interaction occurs, audits the following activities:

- Logins and logouts
- Creation, viewing, copying, or deletion of information
- Changes to (editing) information
- Changes of access restrictions on data
- Use of analysis applications
- Changes in a user's access privileges
- Attempts to access data which have labels that are inconsistent with user privileges (attempted unauthorized access of information)

Audit log entries include the user's unique ID, the action taken, a reference to the data elements acted upon, and a date/time stamp. These audit logs are only available for inspection to the AFI ISSO or their appointed security administrator. Other users are not able to access the audit logs. Audit logs are maintained online for 90 days, and offline for 7 years. On a retroactive basis, should some incident occur, logs can be reviewed after the fact and managers can determine who accessed what information to a certain level of granularity.

The AFI system automatically notifies the ISSO of suspicious events including:

- Downgrading clearance or access restrictions on data
- Changes in a user's access privileges
- Attempts to access data which have labels that are inconsistent with user privileges

The DHS ISSO for AFI is assigned in writing and is required to review the automatic audit logs weekly. Employees are notified that audits are conducted. Warning banners appear at logon to inform users that all activity at every workstation is monitored.

Access to information is also restricted based on user roles. Analysts have access to raw data obtained from the underlying source systems, analytical tools, and have the ability to create projects and law enforcement intelligence products, but consumers (finished intelligence product users) do not. Further, only analysts authorized to access the data in the underlying system have access to that same data through AFI. This is accomplished by AFI passing individual user credentials to the originating system or through a previously-approved certification process in another system. Finally, those users in the consumer role will only have access to finished intelligence products published to the AFI repository and will not have access to raw data or analytical tools.

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

The CBP process owners and all AFI users are required to complete biannual training in privacy awareness. All authorized CBP personnel undergo the privacy training required of all CBP employees with access to CBP's law enforcement systems. This training is regularly updated. Users who do not complete this training will lose access to all computer systems, which are integral to their duties.

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

Only authorized CBP personnel and analysts who require access to the functionality and data in AFI as a part of the performance of their official duties and who have appropriate clearances or permissions will have access to AFI. Initial requests for access to the system are routed from the users through their supervisors to the specific CBP process owners. Need-to-know determinations are made at both the supervisor and process owner levels and background investigation statuses are validated before a profile is created. The user, supervisor, and process owner are notified via email that the request has been processed along with instructions for the initial login. As part of this user validation process, CBP assigns roles and privileges to the user granting access to only those specific functions and specific data needed in performance of the particular user's official duties.

CBP maintains AFI access records showing which users have accessed the system, which functions they have used, and which data they have accessed. AFI managers revoke a user's access when no longer needed or permitted. Account/access retention is monitored by a back-end service that analyzes account creation, access granting, and renewal dates for all users. CBP Information Systems Security Policies Handbook HB 1400-05 mandates periodic supervisory review and revalidation of system accesses of users in order to perform their authorized tasks.

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?

Information sharing agreements, MOUs, new uses of the information, and new access to AFI by organizations within DHS and outside are reviewed and approved by the governance board as described above in the Abstract and Account Access, Audit Controls, and Governance sections.

Responsible Officials

Laurence Castelli
CBP Privacy Officer
Office of International Trade
U.S. Customs and Border Protection
Department of Homeland Security

Jim Gleason
Office of Intelligence and Investigative Liaison
U.S. Customs and Border Protection
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix A – Detailed list of anticipated PII data stored by AFI

Anticipated PII data elements in AFI include:

- Address information including, but not limited to:
  - Street number and name
  - City name
  - Country
  - ZIP Code / Postal Code
- Document information including, but not limited to:
  - Document number
  - Country issuing the document
  - Code of the country that issued the entry document
- Vehicle information including, but not limited to:
  - Conveyance / vehicle make and model code
  - License or tag number of a vehicle
  - License tag description text
- Travel related information including, but not limited to:
  - Arrival/Departure port or location
  - Name of the city that the visa used to be admitted to the U.S. was issued
  - Traveled via country code (ISO)
- Person specific information including, but not limited to:
  - City of birth
  - Country/State of birth
  - Country of citizenship
  - Age
  - Date of birth
  - Name (First and Last, MI)
  - Gender of a person, male or female
  - Marital status code
  - Social Security Number

  - State of residency
  - Race of a person
  - Alias
- Case number
- Designated alien registration file number
- I94 Admission number provided on the admission form
- ID of user that did last update
- IDENT Fingerprint identification number
- Inspector ID number
- Internal person identification number
- Name of the user who created/updated the record
- Officer name
- Officer identification number
- Person ticket number
- Source lookout activity identifier
- Source lookout person identifier
- Source system unique identifier of a person crossing the border
- Surrogate key number for the country that issued the entry document a person used to enter or be admitted to the U.S.
- Surrogate key number for the citizenship country code
- Surrogate key that identifies birth country records in the geography dimension
- Surrogate key that identifies citizenship country records in the geography dimension
- Unique surrogate identifier for agent dimension
- Unique system-assigned surrogate key for this geography dimension record
- Unique TECS ID number
- User ID
- Witness Name

Appendix B – List of Relevant Systems and SORNS, where applicable, for data available through AFI

AFI incorporates records from other government systems, including:

- DHS/CBP-006 Automated Targeting System (ATS) (published May 22, 2012, 77 FR 30297);
- DHS/CBP-005 Advanced Passenger Information System (APIS) (published November 18, 2008, 73 FR 68435);
- DHS/CBP-007 Border Crossing Information (BCI) (published July 25, 2008, 73 FR 43457);
- DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE) (published May 3, 2010, 75 FR 23274) – which covers EID
- DHS/CBP-009 Electronic System for Travel Authorization (ESTA) (published June 10, 2008, 73 FR 32720);
- DHS/CBP-016 Non Immigrant Information System (NIIS) (published December 19, 2008, 73 FR 77739);
- DHS/CBP-013 Seized Asset and Case Tracking System (SEACATS) (published December 19, 2008, 73 FR 77764);
- DHS/ICE-001 Student Exchange and Visitor Information System (SEVIS) (published January 5, 2010, 75 FR 412);
- DHS/CBP-010 TECS (published December 19, 2008, 73 FR 77778);
- DHS/ALL-030 Use of the Terrorist Screening Database System of Records (published July 6, 2011, 76 FR 39408);
- Department of State's Consular Consolidated Database (CCD) PIA available at http://www.state.gov/documents/organization/93772.pdf.