Privacy Compliance Review
of the
U.S. Customs and Border Protection (CBP)
Analytical Framework for Intelligence (AFI)

December 19, 2014

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

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

Table of Contents

I. Background

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP), Office of Intelligence and Investigative Liaison (OIIL) serves as a coordinating facilitator that integrates CBP's diverse intelligence capabilities into a single cohesive intelligence enterprise. OIIL supports CBP's mission through a multi-layered approach that includes collecting and analyzing advance traveler and cargo information, using enhanced law enforcement technical collection capabilities, providing timely analysis of intelligence and information, and establishing intelligence-sharing relationships with Federal, state, local, tribal, and intelligence agencies. OIIL brings together and leverages the expertise of other CBP offices including the Office of Field Operations, Office of Border Patrol, Office of Air and Marine, and Office of Information and Technology (OIT) to execute its mission.

As part of CBP's authority to protect the border and enforce applicable laws at the border, CBP conducts research and analysis on existing data systems to identify potential law enforcement or security risks and develops finished intelligence products (hereinafter referred to as "finished intelligence products" or "products").

In 2012, OIIL developed the Analytical Framework for Intelligence (AFI) to enhance DHS's ability to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and to improve border security. AFI augments DHS's ability to gather and develop information about persons, events, and cargo of interest by creating an index of the relevant data in existing operational systems and providing DHS AFI analysts with tools that assist in identifying non-obvious relationships. AFI allows analysts to generate tactical, operational, and strategic law enforcement 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.

Prior to using AFI for research and analysis, DHS analysts employed dozens of searches or 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. This was an inefficient, time-consuming process. DHS analysts did not have a single access point to identify and analyze relevant data to develop intelligence products. AFI was developed to improve the efficiency and effectiveness of CBP's research and analysis process by providing a platform for research, collaboration, approval, and internal publication of finished intelligence products. DHS AFI analysts use AFI to conduct research on individuals, cargo, or conveyances to understand whether there are patterns that can assist in identifying potential law enforcement or security risks.

AFI indexes information from many different source systems. This allows for a more efficient search because the data from those systems is compiled in a manner that was not previously accessible in one system. It allows DHS AFI analysts to perform link analysis to discover patterns or associations among various entities. The following privacy risks are posed by the compilation of data collected from multiple source data systems:

- *Unauthorized access*: Maintaining an index of data from several different systems in one database may provide users with access to more data than their individual system access rights permit.

- *Inaccurate data*: AFI could retain incorrect information because it draws upon other systems with varying refresh rates, instead of collecting information directly from the original data source.

- *Inconsistent purpose*: The data may not be used consistently with the purpose for which it was originally collected by the source systems.

The DHS Privacy Office and CBP issued a Privacy Impact Assessment (PIA) and System of Records Notice (SORN) for AFI in 2012.[1] Due to the sensitive nature of the AFI system, including its search and aggregation capabilities, AFI was developed in coordination with the DHS Privacy Office to minimize privacy risks. These privacy risks are identified and discussed in the 2012 AFI PIA.

The DHS Privacy Office also required that AFI undergo a Privacy Compliance Review (PCR) within 12 months of the system's operational deployment. The objective of this PCR is to assess compliance with the existing compliance documentation published by AFI and ensure the privacy protections in the PIA are followed. This is the first PCR on the AFI system. Between August 2013 and May 2014, the DHS Privacy Office Oversight Team assessed these privacy protections. To complete this objective, the DHS Privacy Office reviewed the AFI PIA and SORN; reviewed public comments submitted about the AFI SORN; conducted site visits and received briefings from AFI program personnel; developed and administered a questionnaire to the AFI program; reviewed all responses to the questionnaire and provided follow-up questions to the AFI program; reviewed all security incidents for a randomly selected month; and reviewed AFI training and governance documents.

[1] *See* DHS/CBP/PIA-010 Analytical Framework for Intelligence (AFI) Privacy Impact Assessment (June 1, 2012), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_afi_june_2012.pdf and DHS/CBP-017 Analytical Framework for Intelligence System of Records Notice (SORN), 77 FR 33753 (June 7, 2012), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-06-07/html/2012-13813.htm.

II. Scope and Methodology

The DHS Privacy Office conducted a PCR of the AFI system, in coordination with OIIL leadership, the CBP Privacy Office, and representatives of the CBP OIT, for the period of June 2012 through December 2013. To assess AFI's overall compliance with the existing PIA and SORN, the DHS Privacy Office carried out the following activities:

- Reviewed the existing PIA and AFI SORN;
- Reviewed public comments submitted about the AFI SORN;
- Conducted a site visit and received a briefing from the AFI program manager in December 2013;
- Developed and administered a questionnaire to AFI that included questions about:
  - compliance with the Fair Information Practice Principles;
  - overall governance;
  - data tagging; and
  - user and training statistics for the review period;
- Reviewed all responses to the questionnaire and provided follow-up questions to the AFI program in April 2014;
- Reviewed all security incidents for the randomly selected month of November 2013;
- Conducted a second site visit with the AFI program manager and representatives from CBP OIT to discuss technical capabilities of AFI in May 2014;
- Reviewed AFI training documents, including ten (10) Quick Reference Guides for AFI release 6.0 and in-person training talking points;
- Reviewed AFI governance documents, including the AFI Working Group Charter and meeting minutes.

This PCR followed a four-step process for each subsection below. The process involved: 1) a description of the requirements from the AFI PIA and SORN, and the DHS Fair Information Practice Principles, which serve as Department policy for analyzing all DHS programs; 2) our review of the requirements; 3) our findings of compliance or non-compliance based on the review of the requirements; and 4) our recommendations, if applicable.

III. Findings

A. Summary

The DHS Privacy Office finds that CBP OIIL developed AFI with privacy-protective objectives and continues to operate AFI with sensitivity to privacy and data aggregation risks. During the two years since AFI's launch, however, CBP has employed new search, analysis, and storage tools that have consolidated more data than was contemplated during the original privacy analysis in the PIA. Accordingly, the DHS Privacy Office makes sixteen (16) specific recommendations for CBP in order to enhance AFI privacy protections commensurate with AFI's use of these new tools. Our general findings are as follows:

- *Unauthorized access*: AFI has several layers of review and approval to determine both role-based access to the broad data types and underlying source system data within AFI and discretionary access to individual products published by AFI analysts.

- *Inaccurate data*: AFI strives for a near real-time refresh rate of underlying source system data. Where technical constraints make real-time refresh impossible, AFI has employed a risk-based approach to determine which datasets require faster refresh to maintain the highest level of data accuracy within AFI.

- *Inconsistent purpose*: AFI has extensive user access controls; however, the use of a new indexing tool raises new privacy concerns not addressed by the original PIA and SORN for AFI.

Our specific recommendations to CBP for these findings are discussed below. Each recommendation or set of recommendations is preceded by a discussion of the AFI privacy requirements as set out in the AFI PIA and the DHS Fair Information Practice Principles (FIPPs).

B. Users

Requirement: The AFI PIA details the roles and responsibilities of two distinct groups of users, DHS AFI Analysts and Finished Intelligence Product Users. At the time of PIA publication, these were the only two roles available within AFI. Since PIA publication, however, AFI has expanded available user roles.

During the original deployment of AFI, DHS AFI Analysts used the system to obtain a more comprehensive view of data available to CBP, and then analyzed and interpreted the data using the visualization[2] and collaboration tools accessible in AFI. Finished intelligence product users had more limited access to AFI and only viewed the finished tactical, operational, and strategic intelligence products that DHS AFI analysts publish in AFI. They did not have access to the AFI data underlying those products.

Only DHS AFI analysts had access to the analytical tools[3]. The DHS AFI analysts used the data from AFI sources systems either in the analytical tool or in the AFI project space where collaboration with other designated users of the information may occur. The DHS AFI analysts 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.[4] Finished intelligence product users are officers, agents, and employees of DHS who have a need to view the products in the performance of their official duties, and who have appropriate clearances or permissions. When finished intelligence product users access AFI, they may either conduct a search to view finished products or select their subject matter preferences within the system so that only certain finished products – consistent with their preferences – are automatically pushed to their homepage within AFI.

Review: We received a demonstration of how potential users request access to AFI and how User Access Managers and AFI Administrators review the applications and approve or deny access. We also reviewed the AFI User Roles Overview, Summary of AFI Roles, and the Standard Operating Procedures for requesting AFI access (potential new users) and for approving access to AFI (user access managers). We also asked CBP to provide responses to questions detailing credential verification, user roles, user statistics, and user re-certifications.

Findings: The initial deployment of AFI was limited to CBP users. As of December 31, 2013, there are 5,446 users of AFI who are almost equally divided between personnel from Immigration and Customs Enforcement (ICE) and from CBP, with a very few additional users United States Citizenship and Immigration Services (USCIS). The AFI program office has

[2] Visualization tools present data in graphic or other pictorial form to allow analysts to see relationships among data.
[3] Analytical tools allow analysts to perform statistical or other mathematical operations to identify relationships among data.
[4] AFI analysts create "projects" within the AFI workspace to capture research and analysis that is in progress and that may or may not lead to a finished intelligence product or RFI response. Projects are designed to work as collaborative workspaces where information, including documents, images, search results, audio/video files, and other relevant artifacts can be stored and accessed by individuals granted access to a project area. High-level information about a project is available to all AFI users to allow for the discovery of information that may be pertinent to an individual's job responsibilities. Projects differ from the finished intelligence *products* commonly referred to throughout this report.

denied requests for access from the U.S. Coast Guard, Transportation Security Administration, Intelligence and Analysis, and the Office of the Inspector General due to concerns regarding mission compatibility with CBP.

User Roles

The AFI PIA describes only the roles AFI Analyst and Finished Intelligence Product User. Since publication of the PIA, however, the AFI program has updated its user role provisioning to include *three* distinct user roles:

1. Consumer – Consumers are DHS personnel (CBP, ICE, and USCIS users) referred to as the "finished intelligence product users" in the AFI PIA, and have access only for browsing and searching published intelligence products within AFI. Consumers may perform a keyword search of AFI content (the finished intelligence products); they cannot search or access the underlying source data within AFI.

2. Analyst – Analysts (referred to as "DHS AFI Analysts" in the PIA for AFI) are CBP intelligence analysts who create, review, and publish finished intelligence products within AFI. Analysts have the same capabilities of Researchers, but they can also access a link analysis tool directly from AFI. Researchers don't have access to the link analysis tool within AFI because ICE users have their own link analysis tool in a separate ICE system called FALCON.[5]

3. Researcher – The Researcher Role is a new role created for ICE users. Researchers have access to AFI for browsing and searching published intelligence products (as do Consumers); however, Researchers can also search the underlying data sources within AFI and create, review, and publish finished intelligence products within AFI (as can Analysts). These search results are limited to the same results that the Researcher could access in the source systems. If a Researcher does not have access to an AFI source system, results from that system will not populate a Researcher's search results in AFI.

User Security Access Controls

In addition to requesting User Roles, potential users requesting access to AFI must also specify the data-types to which they require access. Note that the different data-types apply to the

[5] For a detailed description of the FALCON system and uses, please *see* DHS/ICE/PIA-032a - FALCON Search & Analysis System (FALCON-SA).

products created within AFI, not the underlying source data.[6] Analysts, upon creation of a product, must mark the product with one or more of the data-type security access controls. Product marking is described in full under subsection (G) "Use Limitation." Data-types within AFI include:

- Unclassified;
- For Official Use Only (FOUO);
- Protected Critical Infrastructure Information (PCII);
- Sensitive Security Information (SSI);
- Law Enforcement Sensitive (LES);
- Passenger Name Record (PNR);
- Bank Secrecy;
- Trade Sensitive Information; and
- U.S. Persons (USPER)

To obtain access to any of this data, individual users submit a request through their User Access Manager, who determines and approves the user security access controls based on the employee's need to know in the normal performance of official duties. Full definitions for all User Security Access Controls are listed in Appendix A.

User Access

AFI access is granted in a two-step process. First, the user's request is approved by his or her AFI User Access Manager. The AFI User Access Manager role is limited to trainers and those tasked with providing access to other users (such as supervisors). The User Access Manager may approve, reject, or request revocation of access. Prior to granting access to AFI, the AFI User Access Manager verifies that the potential user has an active TECS account and has completed the AFI training (either via Webinar or two-day instructor-led class). Once the AFI User Access Manager has approved the request, it is routed to an AFI Administrator for approval. After the AFI Administrator has finalized the approval in the system, the user has access to AFI.

When a user requests access to AFI, he or she must select a User Role (i.e., Consumer, Analyst, or Researcher) and all applicable User Security Access Control(s) (e.g., FOUO or PNR). User Access Managers, typically the user's supervisor, then review and approve the access request. The *User Access Manager – Approving AFI Access Guide* instructs Supervisors to verify TECS access, verify that the User has chosen the correct role, and verify that the user

[6] Unlike the DHS Data Framework (*see* DHS/ALL/PIA-046 DHS Data Framework PIA(s)), the underlying source system data is not tagged by data type prior to indexing in AFI.

has selected the correct User Security Access Control(s). Supervisors are responsible for determining a new user's role based on the user's current position, clearance level, and need-to-know. We note, however, that the *Guide* does not direct Supervisors to the AFI Roles Summary document for assistance in choosing a user role; and, even if it did, the AFI Roles Summary is highly technical and lacks a narrative that would assist Supervisors in determining which user roles their employees need.

Supervisors are directed to the document entitled *AFI User Security Access Definitions* for guidance in approving User Access Security Controls. We find, however, that there are no standards for determining which users should be granted access to specific User Access Security Controls. AFI does not track users by Component Office or mission; therefore it is impossible to tell whether a user who has access to Trade Sensitive Information, for example, has a job function that requires such access. Full discretion rests with the Supervisor and it is impossible to determine whether users have been granted appropriate levels of access.

Recommendation 1: CBP should update the AFI PIA to detail the addition of the Researcher role and the expansion of the AFI user universe to include ICE and USCIS users. The PIA update should describe why the new user components were selected while other components were denied.

Recommendation 2: Supervisors should be given more guidance and training on how to choose the correct roles for their employees. CBP should update the AFI Roles Summary to describe the search and access functions of the Consumer, Research, and Analyst roles (as opposed to just their technical AFI functions) to assist Supervisors in choosing the correct role for their employees.

Recommendation 3: Supervisors and User Access Managers should routinely review employee access to AFI data-types to ensure that users still require their given level of access.

Recommendation 4: AFI does not track users by Component Office or mission; therefore it is impossible to tell whether a user who has access to Trade Sensitive Information, for example, has a job function that requires such access. CBP should develop audit or tracking methods to ensure that users are assigned to appropriate User Security Access Controls.

C. AFI Index and Underlying Source System Data

Requirement: The PIA states that 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 PIA describes how 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 - to reduce the number and volume of individual records that must be reviewed to identify the relevant record. This requirement is a privacy-protective measure required by the DHS Privacy Office to minimize the amount of data aggregated and stored by AFI. As we note below, however, AFI is now using a new tool that creates multiple copies of the data, and thus the PIA is no longer accurate in this regard.

Once an underlying source system deletes or changes the data, AFI will delete or change its data during its next refresh from that system. The PIA states that the indexing engines refresh data from the originating system "periodically." Any changes to source system records, or the addition or deletion of source system records, are to be reflected in corresponding amendments to the AFI index as the index is routinely updated.

Review: We reviewed a list of all source data systems to AFI, including their refresh rates. We reviewed responses from CBP regarding how new data sources are determined and indexed, and we received a demonstration and briefing from the Office of Information Technology about the indexing tool.

Findings: We find that the indexing description in the PIA is no longer accurate. When the PIA was published, AFI used an Oracle search platform. AFI now uses Apache Hadoop, a new, open-source indexing tool that allows a much faster search across multiple datasets, but requires AFI to store multiple copies of all source data in multiple locations. Hadoop provides for shared storage and analysis by replicating the underlying data sources, and storing the replicated data in multiple places to prevent system failure. While it is cheaper and faster than previous search and analysis tools employed by the DHS, Hadoop presents significant privacy challenges as its functionality relies on continuous replication of data.

Despite the speed of Hadoop's search and analysis capabilities, the refresh rates for the underlying source systems have not changed. The target refresh rate for all AFI sources is daily, and the search infrastructure is currently being expanded to support this goal. At present, the source refresh rate depends on the size of the data set to be indexed, and the level of risk posed by data. For example, a data source of inadmissible persons to the U.S. has a faster refresh rate than trade entry information. The load on the system would be crippling if all source systems refreshed in real-time. Source systems generally refresh at night, so as to maintain source system

operation during business hours. Therefore, there remains a privacy risk that information within AFI will be inaccurate until the source systems refresh.

Recommendation 5: CBP should complete Privacy Threshold Analyses (PTA) for all system or program updates that may create new privacy risks to determine whether additional or updated privacy compliance documentation is required. AFI's use of the new Hadoop search and analytics tools requires an update to the AFI PIA, and a thorough analysis of the privacy risks posed by replicating data across multiple storage locations.

Recommendation 6: CBP should continue to strive for a one-to-one refresh rate for all underlying source systems to minimize to the greatest extent possible any discrepancies between the data within AFI and the source data.

D. Transparency

Requirement: The DHS Transparency Principle states that DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII). The AFI PIA states that AFI will publish a SORN to cover the finished intelligence products. However, for the index and analyst created projects, AFI does not collect any information directly from individuals and therefore does not have an opportunity to provide notice of such collection. Commercial data aggregators collect information from publicly available and proprietary records, and therefore do not likely provide notice to the individual prior to collection.

Review: As a law enforcement system, AFI does not collect information directly from individuals and cannot provide notice at the point of collection. However, we reviewed the AFI PIA and the AFI SORN, which are both published on the www.dhs.gov/privacy website and available to the public.

Findings: The AFI SORN was published on June 7, 2012.[7] The SORN, and PIA, were published on the public-facing DHS Privacy Office website prior to the launch of AFI. These documents are designed to provide notice to the public regarding a new or modified collection of information. The AFI SORN details the AFI record source categories, including citations to the SORNs for all CBP and DHS systems used as AFI sources. The AFI SORN also provides notice that AFI accesses records from the following external sources, but that the records are not part of

[7] *See* DHS/CBP-017 – Analytical Framework for Intelligence System, (June 7, 2012) 77 FR 13813, *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-06-07/html/2012-13813.htm.

the index: Department of State; Department of Justice/FBI; Department of Treasury; and commercial information from commercial data providers and geospatial data providers. The SORN also states that 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. The annual DHS Data Mining Report to Congress provides additional notice about the activities of AFI.[8]

Although AFI is a law enforcement system and does not collect information directly from the public, adequate notice is provided through the publication of the PIA and SORN on the DHS public-facing website and the Federal Register. DHS received five (5) non-substantive public comments on the SORN.

Recommendation: We find AFI in compliance with the Transparency requirements and have no recommendations at this time.

E. Individual Participation

Requirement: The DHS Individual Participation Principle states that DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Privacy Act Requests

For AFI index data and source data, as described under Categories of Records in the 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, the SORN states that CBP will provide access to the information maintained in AFI.

Per the AFI PIA, notwithstanding the applicable exemptions, CBP will review all such requests on a case-by-case basis. When 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, CBP may waive the applicable exemption, in accordance with procedures and points of contact published in the applicable SORN.

[8] Please see http://www.dhs.gov/privacy-foia-reports for access to all DHS Privacy Office reports, including the annual Data Mining Report to Congress.

Redress and Correction of Records

The AFI PIA states that data accessed by AFI from source systems may be corrected by means of the processes described in the PIAs for those systems. As AFI draws upon other source systems for its data, any changes to source system records, or the addition or deletion of source system records, the PIA states that those changes will be reflected in corresponding amendments to the AFI index as the index is periodically updated. While individuals do 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.

Review: We requested access to all Freedom of Information Act (FOIA)[9] or Privacy Act requests, and all CBP or ICE responses, for information within the AFI System of Records. We also requested the policy noted in Section 2.4 of the PIA requiring DHS AFI analysts "to make changes to the data records in the underlying DHS system of record if they identify inaccurate data and [to] alert the source agency of the inaccuracy."

Findings: The CBP and ICE Privacy Offices confirmed that no FOIA or Privacy Act Requests have been filed for AFI data as of December 31, 2013. AFI is an exempted system under the Privacy Act. CBP Disclosure professionals must release information from AFI, though exempted from the Privacy Act, as long as there is no exemption for giving access to the record from the underlying source system. We were unable to identify any guidance directing CBP Disclosure professionals of this requirement.

We were also unable to identify a CBP policy that requires DHS AFI analysts to "to make changes to the data records in the underlying DHS system of records if they identify inaccurate data and alert the source agency of the inaccuracy." The near real-time refresh rate of the AFI index from the underlying source data systems reduces the likelihood of inaccuracy, but there is no policy or procedure requiring DHS AFI analysts to update the underlying records.

Recommendation 7: CBP should issue guidance, and provide training, for CBP Disclosure professionals on implementing the requirement to provide access to information maintained in AFI, despite AFI's general exemption from certain provisions of the Privacy Act, if the requested record is not exempted from access in its source system of records.

Recommendation 8: CBP should issue detailed standard operating procedures or rules of behavior that dictate all user requirements, including the requirement in the PIA that DHS AFI analysts make changes to the data records in the underlying DHS system if they identify

[9] 5 U.S.C. § 552.

inaccurate data and [to] alert the source system owner of the inaccuracy. If this is not technically possible, CBP should update the PIA.

F. Purpose Specification

Requirement: The DHS Purpose Specification Principle requires DHS to specifically articulate the authority that permits the collection of PII and the purpose (or purposes) for which the PII is intended to be used for all programs.

Governance

To ensure that AFI was built and used consistent with the authorities of the Department, CBP committed to create a governance body of individuals from OIIL, OFO, the CBP Privacy Office, Office of Chief Counsel, and OIT, who review requested changes to the system on a quarterly basis and determine whether additional input is required.

The governance board, known as the AFI Working Group (AFIWG), directs 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 roles, and new or expanded data to be made available in or through AFI. The governance board reviews and approves all information sharing agreements, MOUs, new uses of the information, and new access to AFI by organizations within DHS.

Mission Compatibility

The PIA states that AFI may only access 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.

Review: We reviewed the AFI Working Group charter, meeting agendas, and meeting minutes. We also requested that AFI program staff describe the process for adding new data sources to AFI. We reviewed the internal AFIWG documentation. The AFIWG Charter has been in draft since April 2012. The draft Charter provides that:

> "[m]embers of the AFIWG will be responsible for: Reviewing, validating, and identifying intelligence and analysis gaps that may be addressed by the AFI system; Prioritizing and de-

conflicting requirements; Defining and approving information sharing agreements; Defining and approving new user roles; Approving inclusion of new data sets and retirement of old data sets; Defining, clearing, and approving new user groups (such as a new external Federal Agency being provided access for the first time); Defining and approving access rules including which groups of users should have access to information only or access to information and data; Acting as liaison and spokesperson for organizational components; and Other activities determined by the AFIWG."

For our review, CBP submitted meeting minutes and agendas from AFIWG meetings in 2012.

Findings: The AFIWG has not convened since September 2012. Based on these documents, it appears that the AFIWG has not been involved in reviewing information sharing agreements, the inclusion of new data sets, or defining new access rules for users. Since AFI's launch in 2012, both ICE and USCIS have been added as users, and the data sets for AFI continue to expand. The AFIWG has not been included in these decisions.

We find that there is an inadequate level of governance to prevent mission creep and ensure that information used by AFI is consistent with the purposes for which it was originally collected. Without regular meetings and consistent attendance, the AFIWG cannot "ensure 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," as the draft AFIWG charter requires.[10]

Recommendation 9: CBP should implement the contemplated governance structure described in the AFIWG Charter. CBP should conduct regular AFIWG meetings, require attendance from AFIWG members, finalize the AFIWG Charter, and document the agendas and outcomes of all meetings.

G. Data Minimization

Requirement: The DHS Data Minimization Principle requires DHS to only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s) of all programs. To meet the data minimization requirements, the AFI PIA describes three privacy enhancements to ensure the minimum amount of data is collected and retained:

[10] AFI Working Group Charter, Draft, 2012.

Minimization

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. Once an underlying source system deletes or changes the data, AFI will delete or change its data during its next refresh from that system.

Retention

AFI is required to adhere to the records retention policies of the source data systems, which furthers data minimization by retaining data only as long as an approved retention schedule permits. When the PIA was published in 2012, AFI was in the process of completing National Archives and Records Administration (NARA) requirements for data retention to obtain a retention schedule. AFI proposed that its retention schedule be the same as the retention schedule presently in place for similar records within the Department. Projects would be retained for up to 30 years, requests for information (RFI) and responses to RFIs would be retained for 10 years, and finished intelligence products would be retained for 20 years.

Recertification

Per the PIA, projects containing PII must be recertified annually or the information must be purged from the AFI system. This furthers data minimization by ensuring that only PII that is relevant and necessary is retained in AFI projects. As noted above, AFI analysts create "projects" within the AFI workspace to capture research and analysis that is in progress and may or may not lead to a finished intelligence product or RFI response. Projects are designed to work as collaborative workspaces where information, including documents, images, search results, audio/video files, and other relevant artifacts can be stored and accessed by individuals granted access to a project area. Projects differ from the finished intelligence *products* commonly referred to throughout this report.

Not all projects become products. Projects can remain open and available for authorized users to view indefinitely. Therefore, the PIA specifies an annual "PII recertification" requirement for all projects. When they create their project, project owners are prompted to select whether the project contains PII. If it does, they are reminded annually to certify (via email) whether or not the project is still active and still requires PII. If the project is no longer active or no longer requires PII, it is purged from the system. A project becomes inactive if the project owner fails to recertify the project, either because the project has been overcome by events or is no longer relevant.

Review: To assess compliance with the data minimization requirements, we reviewed PCR questionnaire responses, reviewed the refresh rates for the index source systems, and received a demonstration of the indexing and recertification capabilities. We reviewed Quick Reference Guides for Products and Projects and training webinar transcripts. We interviewed representatives from OIT to further understand the indexing technology and search methodology.

Findings: AFI was originally designed to minimize the amount of data collected and stored within the AFI system, purposefully leaving the source system records in their original system of collection. In the two years since the publication of the PIA, however, as discussed in subsection (B) "AFI Index and Underlying Source System Data" above, the AFI program made a business decision to use Hadoop, a less privacy-protective technology, to enhance the search and analytic capabilities of the system. Hadoop is considered less privacy sensitive due to the replication of data sets within a new environment, which is principally designed to permit exploitation of the data for analysis and dissemination.

Minimization

We find that the indexing description in the PIA is no longer accurate. When the PIA was published, AFI used an Oracle search platform. AFI now uses Apache Hadoop, a new, open-source indexing tool that allows a much faster search across multiple datasets, but requires AFI to store multiple copies of all source data in multiple locations. Hadoop provides for shared storage and analysis by replicating the underlying data sources, and storing the replicated data in multiple places to prevent system failure. While it is cheaper and faster than previous search and analysis tools employed by the DHS, Hadoop presents significant privacy challenges as its functionality relies on continuous replication of data.

Under the Oracle model, AFI was able to index the underlying source system data, *without retaining a complete copy of the responsive data*. AFI now stores multiple copies of all DHS source system data as a distributed file-system that stores data on multiple machines/servers, providing very high aggregate bandwidth across all connected machines/servers (known as the "cluster").

Retention

AFI is required to adhere to the records retention policies of the source data systems. As described in Subsection B, the target refresh rate for all AFI sources is daily. However, at present, the data source refresh rate is grouped by the size of the data source, and the level of risk posed by data. For example, a data source of inadmissible persons to the U.S. has a faster refresh rate than trade entry information. The load on the system would be crippling if all source systems refreshed in real-time. Most source systems refresh once a day, at night, so as to maintain source

system operation during business hours. Therefore, there remains a privacy risk that information within AFI will be inaccurate until the source systems refresh.

CBP has not completed a retention schedule for AFI.

Recertification

The data maintained in AFI is subject to an annual PII re-certification process, which requires that users recertify any information marked as containing PII to ensure its continued relevance and accuracy. AFI includes the option to certify that a *Project* contains PII, but not a *Product.* Projects are the collaboration workspaces which may or may not produce finished intelligence products. The rationale behind this distinction is that projects stay open and available to authorized users until they are deleted. Products are published as a snapshot in time, and all PII included in a published product was deemed necessary at the time of publication. Should information in a product change or become updated, the Analyst will issue a new product. Projects, however, can stay open indefinitely and are available to any authorized user. The PII recertification process reminds managers that their employees have open projects that contain PII and affords them an opportunity to delete or update these projects if the PII or project is no longer needed.

We reviewed the AFI Quick Reference Guides for Projects and Products, as well as the transcript for AFI user training. The PII-recertification requirement is mentioned once without elaboration in the training transcript. This process is not fully explained to users or supervisors and is not memorialized in policy.

Recommendation 10: The use of the new Hadoop search and analytics tools requires an update to the AFI PIA, and a thorough analysis about the privacy risks posed by replicating data across multiple storage locations. (Note this is same Recommendation from Subsection B.)

Recommendation 11: CBP should continue to strive for a one-to-one refresh rate for all underlying source systems to obviate any inaccuracies between the data within AFI and the source data. (Note this is same Recommendation from Subsection B.)

Recommendation 12: CBP must identify or complete a records retention schedule for AFI data with NARA.

Recommendation 13: CBP should update policies and training materials to ensure that supervisors and users understand the PII recertification process and requirements.

H. Use Limitation

Requirements: The most privacy-protective requirements in the PIA for AFI are (1) adherence to the user access controls of the source data systems and (2) the use of Product tagging to create user security access controls for products within AFI. These requirements ensure that CBP will use PII solely for the purpose(s) specified in the source system notice at the time of original information collection.

Inappropriate Access to Source Data Systems

A considerable 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 access rights to individual systems permit. To mitigate this risk, the source system that originally collected the data maintains control of that data even though the data is co-located in both the source system and in AFI. Accordingly, only 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.

Access Controls for AFI Products

Analysts must designate the appropriate user security access control 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. Analysts must mark or tag intelligence products containing PII prior to publication to the system. The marking ensures that only those finished intelligence product users who 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.

The document tags are used to narrow down the search for a finished intelligence product and 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 in AFI.

External Sharing

The PIA states that 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 AFI SORN.

Review: We received a demonstration of the user log-in process, a briefing from OIT on the user credential verification application, or "AppAuth," process at DHS, and reviewed all product marking options. We also tested the search capability within AFI to verify whether search results matched the product markings.

Findings: In general, controls developed by AFI promote the principle of use limitation, and they are functioning as described in the PIA.

Access to AFI source data systems

We find that AFI applies a security role for access to every data source, preventing users who do not have access to the underlying source system from accessing it through AFI. For sources that provide a direct interface capability, AFI queries the source system, sending the user's log-in information or other user information to verify the user has access at the time of login to AFI.

User credentials are not passed from a source system into AFI. AFI accepts only user credentials from a DHS browser running within the DHS OneNet, meaning that a user must be on the DHS internal network prior to accessing AFI. User credentials are then validated by the DHS "AppAuth" infrastructure, which is a common way to verify credentials throughout the Department without passing user log-in information system by system. AppAuth is linked to the user's Active Directory[11] entry and stores the log-in credentials and approvals for DHS systems that the user has been approved to access. Due to this configuration, it is impossible for users to use AFI as a workaround to access underlying data sources for which they do not have authorized access.

Access Controls for AFI Products

Access to AFI products is controlled in two ways: 1) user preferences and product metadata and 2) User Access Security Controls (described in subsection IV.A). Users set preferences based on the areas of interest their jobs require (for example, drug smuggling or northern border related products). They can create custom views to display products that meet their preferences. They can select products based on metadata and/or a keyword.[12] Users can also receive email notifications when a product is published that matches their preferences. Though metadata serves no technical access control function, it serves as a functional access control to

[11] The Active Directory is the Global Address List for DHS, containing work contact information for all employees.
[12] Metadata within AFI means additional data tags that a product publisher adds to the product to ease searchability. These metadata tags serve no access control function and are only used to assist users in finding relevant products. Metadata examples include: Reporting Location, Author, Published Date, Areas, Subjects, Category, Keyword.

assist users in finding and viewing only products that are relevant to their job needs. Therefore, users do not search through irrelevant products.

When they create a product, analysts must mark it with one or more of the data-type User Security Access Controls discussed above.

Search results will display only the products that meet a user's User Access Security Controls. If a user does not have access to Trade Sensitive Information, for example, he or she will never see any search results that have been marked by the Product Publisher as Trade Sensitive Information. Supervisors are responsible for approving their employees requested access to data-types within AFI. As noted in subsection A), supervisors are directed to the *AFI User Security Access Definitions* document for guidance in approving User Access Security Controls.

External Sharing

At the time of this PCR, AFI is not used to share information outside of DHS; nor is AFI used to track or respond to RFIs, as described in the PIA. CBP may transition its RFI response, storage, and tracking system to AFI in the future.

Recommendation: We find AFI in compliance with the Use Limitation requirements and have no recommendations at this time.

I. Data Quality and Integrity

Requirements: The DHS Data Quality and Integrity Principle requires DHS to, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete. The PIA states that to ensure data quality and integrity, AFI periodically refreshes the index, requires recertification of all products containing PII, requires workspace collaboration and peer review among analysts, and has developed policies for the recall and correction of products that contain erroneous information.

Index Refresh

Per the PIA, AFI's index periodically 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 an 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 AFI users. Additionally, when an Analyst conducts a query, any changes, additions, or deletions of records from commercial data aggregators will be reflected in that query.

PII Recertification

The data maintained in AFI is subject to an annual PII re-certification process, which requires that users recertify any 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.

Analyst Workspace Collaboration

DHS AFI analyst-provided information is stored in Projects, collaborative workspace(s) where other analysts can review and challenge it. Finished intelligence products, and products in draft, are subject to peer and supervisor review to ensure accuracy before publication in AFI. In addition, 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 Analysts are responsible for the integrity of the data they provide. Should an Analyst enter erroneous information, he or she is required to correct the entry immediately upon determining it to be incorrect. This requirement applies to any data to which an Analyst has access, not just data provided by the Analyst. DHS AFI analysts are also 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 system owner 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.

Erroneous products

At times, erroneous information may be published in a finished intelligence product. When incorrect information is discovered, a revised product will be published in AFI to correct the information or to note the questionable fact or content, and the incorrect product will be removed from the AFI repository. For any products that were published 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.

Review: We interviewed representatives from OIT and received a demonstration of the AFI auditing capabilities. We reviewed responses to the AFI questionnaire, and conducted test searches with CBP personnel.

Findings: We find that, AFI has employed tools and technical controls to maintain a high level of data quality within the system. As AFI is a law enforcement system with considerable search and analysis functions, it is imperative that data be as accurate and timely as possible.

Index Refresh

As noted in subsection B), the data source refresh rate is grouped by the size of the data source, and the level of risk posed by data. For example, a data source of inadmissible persons to the U.S. has a faster refresh rate than trade entry information. The load on the system would be crippling if all source systems refreshed in real-time. Source systems refresh at night, so as to maintain source system operation during business hours. From a data quality and integrity perspective, while we would prefer a real-time source system refresh rate to reduce the possibility of inaccurate or outdated data in AFI, we find that AFI's risk-based approach promotes acceptable data quality.

PII Recertification

When creating a project, Analysts are presented with an option asking if PII is contained in the project. Analysts must mark a box certifying that the project contains PII. This starts an internal "clock" that will prompt the user in one year to re-certify whether the project is still active and needs PII. AFI automatically sends the project owner an email annually. The project owner must certify whether the project is still needed; and if the project is not recertified, it will be purged from the system.

Analyst Workspace Collaboration

AFI has created sub-roles within the Analyst and Researcher roles that promote the peer review process to ensure accuracy. Prior to product publication, a product must be reviewed by a Product Manager and the Product Publisher, whose roles differ from that of the Product Author. Typically, Product Managers and Product Publishers are Supervisors or Team Leaders, whereas Product Authors are typically non-supervisory intelligence or law enforcement analysts.

Erroneous products

We asked CBP to describe the process AFI follows for correcting, amending, or redacting products that have been found to be inaccurate. Products in AFI are managed by users who have been granted the Product Publisher user role, which allows them to publish an approved Intelligence Product. This role also allows users to edit product metadata, quick publish (publishing of externally approved products), and un-publish (retract) published products.

Since AFI's inception and through December 31, 2013, CBP has published 1,202 products and ICE has published 510 products in AFI. AFI does not keep metrics for the numbers of products that have been corrected or un-published. Un-published products are never deleted. If a Product Publisher determines that a published product was inaccurate, he or she can un-publish the product to remove it from the search capability. While the un-published products are no

longer visible in the AFI search, they can be revived by the author and put through the publish workflow again.

This functionality is managed by Product Publishers. A published product can be un-published and corrected. The product can then be re-sent through the publishing notification process to be posted. This process is not documented in any training materials or quick reference guides provided to the DHS Privacy Office.

Recommendation 14: CBP should update training and policies to explain the un-publishing process and why/when a product should be un-published. CBP should consider creating a notification process to alert users when information in a product is outdated or has been superseded by a new product, to reduce reliance on old or outdated information.

J. Security

Requirements: The Security Principle requires DHS to protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. When the PIA was published, the Certification & Accreditation (C&A) of AFI was pending. AFI employs the following security measures:

- All AFI users must consent to monitoring or they cannot use the system.
- 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 Sensitive But Unclassified (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).

Review: We reviewed the consent to monitoring (available to all users prior to AFI log-in), we verified the status of the C&A for AFI, and we verified the RBAC and DAC, described in full in

the subsection (A) "Users" and subsection (B) "AFI Index and Underlying Source System Data" above.

Findings: The security posture for AFI meets the privacy requirements to prevent loss, unauthorized use, and disclosure of information. On April 12, 2013, AFI received an Authority to Operate (ATO) that is valid until April 12, 2016. AFI has posted a notice of consent to monitoring for all users. The RBAC are discussed in detail in subsection A) Users, above. The DAC are met by the product tagging, user preferences, and metadata tools available for AFI users to further restrict the dissemination of information to authorized persons.

Recommendation 15: During the next PIA update, AFI should update the PIA to include the completion of the Certification and Accreditation for the system and should fix the error in the list of data-labelling options that lists "PII," rather than USPER, as a User Access Security Control type.[13]

K. Accountability and Auditing

Requirements: The Accountability and Auditing principle requires DHS to mitigate 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.

AFI Search Results

AFI stores all users search parameters but not the search results themselves. AFI logs all search terms, so that users can re-run searches against new data in AFI following an underlying source data refresh.

Suspicious Events

The AFI system automatically notifies the Information System Security Officer (ISSO) of suspicious events including: 1) downgrading clearance or access restrictions on data; 2) changes in a user's access privileges; and 3) attempts to access data that have labels that are inconsistent with user privileges. AFI managers revoke a user's access when no longer needed or permitted.

[13] From an Intelligence Community perspective, PII, as a data description, is not a limitation in the same manner that "USPER" is. EO 12333 imposes restrictions on access and use of USPER data that goes well beyond the general safeguarding and security required for PII. Most of the relevant information in AFI contains PII, so as a label it is less distinguishing.

Account/access retention is monitored by a back-end service that analyzes account creation, granting of access, and renewal dates for all users.

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. 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.

In addition to policy and technical safeguards, the PIA requires the DHS Privacy Office to conduct a privacy compliance review within 12 months of AFI's deployment.

Review: To assess compliance with auditing and accountability controls within AFI, we reviewed a sample of all suspicious events for November 2013, reviewed responses to the AFI questionnaire, and received a demonstration of the system's auditing capabilities.

Findings: We find that generally, AFI has adequate auditing and accountability controls built into AFI. The biggest compliance gap is the lack of storage of the search *results* in the auditable search logs. Search parameters alone are helpful to the user (so they don't have to retype a common search each time); however, without the search results, an auditor or investigator cannot tell what the user actually viewed and possibly relied upon.

AFI Search Results

As noted above, AFI stores the search parameters in auditable logs for all users, but not the search results. Therefore, it is impossible to see what the user actually viewed (and possibly relied upon) from those original search results. Absent the ability to view what the user viewed, it is impossible to determine what information a user relied upon when drafting or commenting on a project or product. If the underlying information was inaccurate, or used in an inappropriate manner, there is no auditable event to determine where the mistake was made.

User Account Re-certifications and Audit

Individual users are annually notified electronically to re-certify their need for access and appropriate User Security Access Controls based on their current job functions. Once a user completes the re-certification request, the request is routed to his or her User Access Manager for approval – a prerequisite for continued access to AFI. The system captures all of these actions in the user provisioning log.

As of December 31, 2013, 126 re-certifications have occurred. To maintain access to AFI and keep their accounts active, users must access AFI at least once every 45 days; otherwise, the account goes into suspension, which requires action by the user and the designated AFI User Access Manager to reactivate. There is no process for removal of users from the system, even if their access is terminated. The AFI program determined that there is a business need to archive all users for historical purposes. Therefore, the User Access Managers have the ability to set an account to "inactive" but will not delete the account.

Suspicious Events

The AFI ISSO is automatically notified of suspicious information security events. These are detailed in the System Security Plan for AFI as part of the Certification and Accreditation completed on April 1, 2013. We reviewed the suspicious events for November 2013. There were three suspicious events, all of which concerned an external entity trying to inappropriately access AFI from outside of the DHS network.

Auditable Search Logs

As noted in subsection H ("Data Quality and Integrity") above, AFI stores search parameters in auditable logs for all users, but not the search results. We viewed demonstrations of the following auditable capabilities of AFI: a) user logins and logouts, b) creation, c) viewing, copying, or deletion of information through the project history page, d) project deleted pages, e) product publish history pages, f) product workflow history pages, and g) search history archives.

We also reviewed the process for changes to access restrictions of AFI data. AFI logs all user profile changes, including user access roles and user security access controls. All changes to a user's access privileges are logged in the user's profile and are auditable. A change in rights to access a particular a project page is logged as a change to the project. Attempts to access data that have labels that are inconsistent with user privileges (attempted unauthorized access to information) are not audited by AFI, because the user is not given the opportunity to access unauthorized data sources from within the application.

Recommendation 16: CBP should update the audit capabilities in AFI to include not only the search parameters but also the search results for all searches.

IV. Conclusion

The DHS Privacy Office continues to work collaboratively with CBP OIIL to ensure implementation of AFI in a privacy-sensitive manner. The AFI program worked diligently with the DHS Privacy Office to create privacy protective enhancements to the AFI system during development in 2011-2012, and we appreciate AFI's diligence in responding to this PCR. The sensitive nature of the AFI system, the large amount of underlying source system data, and the rapidly changing analytical tools available, require regular AFI privacy compliance reviews.

The DHS Privacy Office recommends that CBP take the following steps to continue to improve its ability to demonstrate compliance with privacy requirements:

- *Recommendation 1*: CBP should update the AFI PIA to detail the addition of the Researcher role and the expansion of the AFI user universe to include ICE and USCIS users. The PIA update should describe why the new user components were selected while other components were denied.

- *Recommendation 2*: Supervisors should be given more guidance and training on how to choose the correct roles for their employees. CBP should update the AFI Roles Summary to describe the search and access functions of the Consumer, Research, and Analyst roles (as opposed to just their technical AFI functions) to assist Supervisors in choosing the correct role for their employees.

- *Recommendation 3*: Supervisors and User Access Managers should routinely review employee access to AFI data-types to ensure that users still require their given level of access.

- *Recommendation 4*: AFI does not track users by Component Office or mission; therefore it is impossible to tell whether a user who has access to Trade Sensitive Information, for example, has a job function that requires such access. CBP should develop audit or tracking methods to ensure that users are assigned to appropriate User Security Access Controls.

- *Recommendation 5*: CBP should complete PTAs for all system or program updates that may create new privacy risks to determine whether additional or updated privacy compliance documentation is required. AFI's use of the new Hadoop search and analytics tools requires an update to the AFI PIA, and a thorough analysis of the privacy risks posed by replicating data across multiple storage locations.

- *Recommendation 6*: CBP should continue to strive for a one-to-one refresh rate for all underlying source systems to minimize to the greatest extent possible any discrepancies between the data within AFI and the source data.

- *Recommendation 7:* CBP should issue guidance, and provide training, for CBP Disclosure professionals on implementing the requirement to provide access to information maintained in AFI, despite AFI's general exemption from certain provisions of the Privacy Act, if the requested record is not exempted from access in its source system of records.

- *Recommendation 8:* CBP should issue detailed standard operating procedures or rules of behavior that dictate all user requirements, including the requirement in the PIA that DHS AFI analysts make changes to the data records in the underlying DHS system if they identify inaccurate data and [to] alert the source system owner of the inaccuracy. If this is not technically possible, CBP should update the PIA.

- *Recommendation 9*: CBP should implement the contemplated governance structure described in the AFIWG Charter. CBP should conduct regular AFIWG meetings, require attendance from AFIWG members, finalize the AFIWG Charter, and document the agendas and outcomes of all meetings.

- *Recommendation 10*: The use of the new Hadoop search and analytics tools requires an update to the AFI PIA, and a thorough analysis about the privacy risks posed by replicating data across multiple storage locations.

- *Recommendation 11*: CBP should continue to strive for a one-to-one refresh rate for all underlying source systems to obviate any inaccuracies between the data within AFI and the source data.

- *Recommendation 12*: CBP must identify or complete a records retention schedule for AFI data with NARA.

- *Recommendation 13*: CBP should update policies and training materials to ensure that supervisors and users understand the PII recertification process and requirements.

- *Recommendation 14*: CBP should update training and policies to explain the un-publishing process and why/when a product should be un-published. CBP should consider creating a notification process to alert users when information in a product is outdated or has been superseded by a new product, to reduce reliance on old or outdated information.

- *Recommendation 15*: During the next PIA update, AFI should update the PIA to include the completion of the Certification and Accreditation for the system and should fix the error in the list of data-labelling options that lists "PII," rather than USPER, as a User Access Security Control type.

- *Recommendation 16*: CBP should update the audit capabilities in AFI to include not only the search parameters but also the search results for all searches.

We discussed these recommendations with AFI program officials, CBP Privacy Office staff, and the DHS Privacy Office Compliance Team, who are taking steps to implement them. The DHS Privacy Office will conduct a follow-up PCR twelve (12) months from the publication of this PCR to assess the status of the recommendations.

V. Privacy Compliance Review Approval

Responsible Official

James Gleason
Director, Intelligence and Advanced Analytics
Office of Intelligence and Investigative Liaison
U.S. Customs and Border Protection

Approval Signature

Original signed copy on file with the DHS Privacy Office.

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

Appendix A: AFI User Security Access Control Definitions

The following definitions assist users in determining which options to select in the "User Security Access" section of the AFI access request form. "User Security Access" impacts the products a user will be able to access in AFI IntelView.

- AFI Users: Select the Security Access options for the types of data that you have a need to know in the normal performance of your daily duties.

- AFI Supervisors: Approve the Security Access options for the types of data that your personnel have a need to know in the normal performance of their daily duties.

For Official Use Only (FOUO): The term used within DHS to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. Information impacting the National Security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 12958, "Classified National Security Information," as amended, or its predecessor or successor orders, is not to be considered FOUO. FOUO is not to be considered classified information.

Products that are identified as FOUO upon uploading into AFI (based on designation of the product itself as FOUO in the product creation process) will have the FOUO checkbox checked. Only users that have a need to know for FOUO information in the normal performance of their daily duties will have access to information identified as FOUO.

Protected Critical Infrastructure Information (PCII): Critical infrastructure information (as defined in 6 U.S.C. § 131(3)), means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. Protected Critical Infrastructure Information is a subset of CII that is voluntarily submitted to the Federal Government and for which protection is requested under the PCII program by the requestor.

Products that are identified as PCII upon uploading into AFI (based on designation of the product itself as PCII in the product creation process) will have the PCII checkbox checked. Only users that have a need to know for PCII information in the normal performance of their daily duties will have access to information identified as PCII.

Sensitive Security Information (SSI): Sensitive security information (SSI), as defined in 49 CFR Part 1520, is a specific category of information that requires protection against disclosure. 49 U.S.C. § 40119 limits the disclosure of information obtained or developed in carrying out

certain security or research and development activities to the extent that it has been determined that disclosure of the information would be an unwarranted invasion of personal privacy; reveal a trade secret or privileged or confidential commercial or financial information; or be detrimental to the safety of passengers in transportation.

Products that are identified as SSI upon uploading into AFI (based on designation of the product itself as SSI in the product creation process) will have the SSI checkbox checked. Only users that have a need to know for SSI information in the normal performance of their daily duties will have access to information identified as SSI.

Law Enforcement Sensitive (LES): The designation used to protect information compiled for law enforcement purposes. LES is a subset of FOUO.

Products that are identified as LES upon uploading into AFI (based on designation of the product itself as LES in the product creation process) will have the LES checkbox checked. Only users that have a need to know for LES information in the normal performance of their daily duties will have access to information identified as LES.

Passenger Name Record (PNR): A record in the database of a Computer Reservation System (CRS) that contains the itinerary for a passenger or a group of passengers traveling together. A PNR typically contains more information of a sensitive nature, including the passenger's full name, date of birth, home and work address, telephone number, e-mail address, credit card details, IP address if booked online, as well as the names and personal information of emergency contacts.

Products that are identified as PNR upon uploading into AFI (based on designation of the product itself as PNR in the product creation process) will have the PNR checkbox checked. Only users that have a need to know for PNR information in the normal performance of their daily duties will have access to information identified as PNR.

Bank Secrecy: The United States' Bank Secrecy Act (or BSA) requires financial institutions to assist government agencies to detect and prevent money laundering. Specifically, the act requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities.

Products that are identified as Bank Secrecy upon uploading into AFI (based on designation of the product itself as Bank Secrecy in the product creation process) will have the Bank Secrecy checkbox checked. Only users that have a need to know for Bank Secrecy information in the

normal performance of their daily duties will have access to information identified as Bank Secrecy.

Trade Sensitive Information: The designation is used for information pertaining to U.S. Trade Policy, strategies and negotiating objectives. Products that are identified as Trade Sensitive upon uploading into AFI (based on designation of the product itself as Trade Sensitive in the product creation process) will have the Trade Sensitive checkbox checked. Only users that have a need to know for Trade Sensitive information in the normal performance of their daily duties will have access to information identified as Trade Sensitive.

U.S. Persons: This designation is used to identify products or information that would need additional review prior to release to elements of the Intelligence Community, due to the inclusion of specific identifying characteristics of U. S. Persons in the product or information.

Title 50 U.S.C. and Executive Order 12333 define U.S. Persons as:

- a citizen of the United States,
- an alien lawfully admitted for permanent residence,
- an unincorporated association with a substantial number of members who are citizens of the U.S. or are aliens lawfully admitted for permanent residence, or
- a corporation that is incorporated in the U.S. except for a corporation directed and controlled by a foreign government or governments.

Products that are identified as U.S. Persons upon uploading into AFI (based on designation of the product itself as U.S. Persons in the product creation process) will have the U.S. Persons checkbox checked. Only users that have a need to know for U.S. Persons information in the normal performance of their daily duties will have access to information identified as U.S. Persons.