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

December 6, 2016

Contact Point
Mario Medina
Director, Targeting Business Division
U.S. Customs and Border Protection
U.S. Department of Homeland Security
(202) 325-1014

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
U.S. 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) Analytical Framework for Intelligence (AFI) is an analyst-oriented, web-based application that augments CBP's ability to gather and develop information about persons, events, and cargo of interest by enhancing search and analytical capabilities of existing data systems.

AFI provides an intelligence platform to support and enhance the Department's ability to:

1. identify individuals, associations, or relationships that may pose a potential law enforcement or security risk; target cargo that may present a threat; and assist intelligence product users in the field to prevent the illegal entry of people and goods, or identify other violations of law;
2. conduct additional research on persons or cargo to detect trends, patterns, and emerging threats, and identify non-obvious relationships between persons, events, and cargo to generate tactical, operational, and strategic law enforcement intelligence products; and
3. share 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, or share externally pursuant to routine uses in the AFI System of Records Notice (SORN).

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"). CBP currently utilizes transaction-based systems such as TECS (not an acronym) and the Automated Targeting System (ATS) for targeting and inspections. AFI provides a set of analytical tools that include advanced search capabilities into existing DHS data sources (and federated queries to other federal agency sources and commercial data aggregators) to allow analysts to search several databases simultaneously. AFI tools present the results to the AFI analyst in a manner that allows for easy visualization and analysis. AFI creates an index of the relevant data in existing operational DHS source systems by ingesting this data from source data systems, as described below, in order to enable a faster return of search results. AFI also permits AFI analysts to upload, index, and store information that may be relevant from other sources, such as the Internet (including social media) or traditional news media, and to document the specific sources of that information.

The DHS Privacy Office and CBP issued a Privacy Impact Assessment (PIA) and SORN for AFI in 2012. 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. The DHS Privacy Office also required that AFI undergo a Privacy Compliance Review (PCR) within 12 months of the system's operational deployment to assess compliance with the existing compliance documentation published by AFI, and to ensure the privacy protections in the PIA were followed. The first PCR[1] on the AFI system was published on December 19, 2014, which reviewed AFI from August 2013 to May 2014, and resulted in 16

[1] https://www.dhs.gov/publication/privacy-compliance-review-analytical-framework-intelligence.

recommendations to enhance AFI privacy protections commensurate with its use. The 2014 PCR also noted that the DHS Privacy Office would conduct a follow-up PCR twelve months from publication to assess the status of those recommendations.

On January 20, 2016, the DHS Privacy Office launched its second PCR of AFI by developing and administering a questionnaire to the AFI program that covered operations from May 2014 to March 2016. The 2012 AFI PIA underwent revisions during the course of the PCR, which impacted the timeline of our review and outcomes of our findings. To complete this PCR, the DHS Privacy Office reviewed privacy compliance[2] and usage documentation; developed an extensive questionnaire, reviewed all responses to the questionnaire, and provided follow-up questions to the AFI program office; reviewed AFI training and governance documents; and conducted site visits with and received briefings from AFI program personnel.

II. Scope and Methodology

The DHS Privacy Office conducted a PCR of the AFI system, in coordination with CBP's National Targeting Center (NTC) leadership, the CBP Privacy and Diversity Office, and representatives of the CBP Office of Information Technology, for the period of May 2014 through March 2016. To assess AFI's implementation of the 2014 PCR recommendations and assess overall compliance with Privacy Policy Guidance Memoranda 2008-01/Privacy Policy Directive 140-06[3] on the Fair Information Practice Principles and the existing PIA and SORN, the DHS Privacy Office carried out the following activities:

- Reviewed findings from the December 2014 PCR;
- Reviewed the 2012 PIA and AFI SORN[4] and 2016 PIA update[5];
- Reviewed August 2015 Privacy Threshold Analysis (PTA);
- Reviewed January 2015 AFI *User Administration Guide;*
- Reviewed DHS Office of the Inspector General (OIG) September 2, 2015 AFI report[6];
- Developed and administered a questionnaire in January 2016 to AFI that included questions about:
    - implementation of December 2014 PCR recommendations,
    - compliance with the Fair Information Practice Principles,
    - overall governance,
    - user vetting and approval,
    - data tagging, and
    - user and training statistics for the review period;

[2] 2012 PIA and SORN, as well as updated PIA finalized on September 1, 2016.
[3] https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles.
[4] At the time of review, the June 2012 AFI PIA (DHS/CBP/PIA-010), available at https://www.dhs.gov/publication/analytical-framework-intelligence-afi, and SORN (DHS/CBP-017), available at https://www.gpo.gov/fdsys/pkg/FR-2012-06-07/html/2012-13813.htm, were the compliance documents in question.
[5] https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-010-a-afi-2016.pdf.
[6] https://www.oig.dhs.gov/assets/Mgmt/2015/OIG-15-137-Sep15.pdf.

- Reviewed all responses to the questionnaire and provided follow-up questions to the AFI program in February 2016;
- Conducted a site visit and received a briefing from the AFI program manager in February 2016;
- Conducted follow up conversations to discuss technical capabilities of AFI in March and April 2016;
- Reviewed AFI training documents, including TECS privacy training and Quick Reference Guides for AFI release 16.2; and
- Reviewed AFI Working Group (AFIWG) Charter.

As the 2012 privacy compliance documents were undergoing revisions during the review period, the focus of the 2016 PCR assessed implementation of recommendations from the December 19, 2014 PCR, and considered program activities against the DHS Fair Information Practice Principles[7] (FIPPs), which serve as Department policy for analyzing all DHS programs. The AFI PIA was updated and finalized on September 1, 2016, impacting the final findings of this PCR. This report discusses the DHS Privacy Office review of AFI against these requirements and our recommendations, if applicable.

III. Findings

A. Summary

The DHS Privacy Office finds that CBP continues to operate and manage AFI with privacy-protective objectives, and with sensitivity to privacy and data aggregation risks. Of the 16 recommendations made in the 2014 PCR, the DHS Privacy Office notes that CBP fully implemented ten and is in the process of implementing the remaining six. The DHS Privacy Office strongly encourages full implementation of the 2014 recommendations and additionally recommends that CBP implement the following eight recommendations to continue to improve its ability to demonstrate compliance with privacy requirements:

Recommendation 1: When User Access Managers and AFI Administrators seek annual AFI access recertification, Managers and Administrators should receive a copy of and affirm their awareness of their responsibilities within the *AFI User Administration Guide*.

Recommendation 2: Recognizing that CBP is drafting a comprehensive intelligence products SORN that will identify AFI's purpose, the individuals and records covered in AFI, and AFI's routine uses, this SORN should be finalized by the end of Fiscal Year 2017. The intelligence product SORN should also reflect changes in user roles, categories of individuals covered by the system, categories of records in the system, routine uses of records maintained in the system, and the data retention schedule.

[7] Privacy Policy Guidance Memoranda 2008-01/Privacy Policy Directive 140-06.

Recommendation 3: CBP should conduct regular AFIWG meetings and fully implement the governance structure, responsibilities, and procedures described in the AFIWG Charter.

Recommendation 4: The AFIWG should monitor and report on implementation of all PCR recommendations and provide regular updates to the DHS Privacy Office with documentation showing corrective actions are completed.

Recommendation 5: CBP must work with the DHS Records Management Office to complete a records retention schedule for law enforcement intelligence products.

Recommendation 6: CBP should continue to work toward an hourly 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: While the annual recertification emails are timely, additional instructions should be added within these emails to explain to project owners what is required of them and memorialized in policy.

Recommendation 8: CBP should update training and policies to explain the un-publishing process and why/when a product should be un-published.

Below is a discussion of each FIPP requirement, how the DHS Privacy Office reviewed AFI for compliance, our findings, and our specific recommendations to CBP for these findings.

B. Use Limitation

Requirement: The Use Limitation FIPP requires that personally identifiable information (PII) be used solely for the purpose(s) specified in notice documentation. This can be analyzed for compliance by the types of users authorized to use the PII for official purposes. The 2012 AFI PIA and 2016 AFI PIA update detail the roles and responsibilities of three authorized groups of AFI users: Analysts, Consumers, and Researchers.

Users

While the June 2012 AFI PIA and SORN describe only the roles of AFI Analyst and Finished Intelligence Product User, the September 2016 PIA updates these roles to Analyst and Consumer respectively, and adds the Researcher role, which allows certain non-CBP authorized users to search data sources and access intelligence products.

As discussed in the 2014 PCR, DHS AFI Analysts are CBP users that use the system to obtain a more comprehensive view of data available and then analyze and interpret the data using the visualization[8] and collaboration tools accessible in AFI. Analysts create, review, and publish finished intelligence products using only the source system data that they already have

[8] Visualization tools present data in graphic or other pictorial form to allow analysts to see relationships among data.

authorized access to. The fewest number of authorized users are assigned this role. All Analysts also have the Researcher role (discussed below). The two roles are functionally equivalent, however the Analyst role is reserved for CBP AFI users who may require a specific tool within the system to complete their job function. (AFI does not currently use any CBP-specific analytic tools.)

Consumers are DHS personnel that have access only for browsing and searching published intelligence products within AFI. Consumers have more limited access to AFI than the other data access roles, meaning they may view finished intelligence products published in AFI IntelView, but Consumers cannot access the research space or analytic tools. Consumers may perform a keyword search of AFI content (products), but they cannot search or access the underlying source data within AFI. The Consumer role has the least degree of access within AFI.

The new Researcher role allows non-CBP users to perform complex data searches across any data source to which they have access and review intelligence products. Researchers use AFI to obtain a more comprehensive view of data available to CBP, and then analyze and interpret the data using the visualization and collaboration tools accessible in AFI. Researchers have access to AFI for browsing and searching published intelligence products (as do Consumers); however, unlike Consumers, 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 they have authorized access to, meaning that, if a Researcher does not have access to an AFI source system, results from that system will not populate in a Researcher's search results in AFI.

In addition to the additional user role, the August 2015 AFI PTA discusses the proposed addition of new user groups within DHS. The AFI PTA identifies the following specific DHS Component offices as having the appropriate authority to warrant access to AFI to assist in the identification of individuals who pose potential security risks and aid in the enforcement of immigration, customs, or transportation security laws and regulations: U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) and ICE Enforcement and Removal Operations (ERO), United States Citizenship and Immigration Services (USCIS) Fraud Detection and National Security (FDNS), U.S. Coast Guard (USCG) Office of Intelligence, Transportation and Security Administration (TSA) Office of Intelligence and Analysis (OIA), and the DHS Office of Intelligence and Analysis (I&A). While these offices have been identified, with the exception of ICE HSI and ERO, and a few pilot users in USCIS FDNS and I&A, the other user groups listed have not yet been granted access to AFI. The September 2016 AFI PIA update goes further to discuss the expansion of authorized users to members of the DHS Intelligence Enterprise[9] (IE), with approval from the AFIWG, AFI's governance and oversight mechanism discussed below. The PIA's Appendix A: Approved AFI External Users, lists all approved non-CBP users who have been granted access to AFI, with approval of the AFIWG, and confirms that this Appendix will be updated as new users are approved. Regardless, users

[9] See DHS Directives System Instruction Number: 264-01-001 Revision Number: 00 Issue Date: 6/28/2013.

from these offices must still individually demonstrate a need-to-know and complete the required application process to obtain AFI access.

User Security Access Controls

When a new user requests access to AFI, the applicant must also specify all applicable user security access controls, which will grant a user the ability to access underlying source data within AFI, as appropriate.[10] Note that the different data-types apply to the products created within AFI, not the underlying source data.[11] Analysts, upon creation of a product, must mark the product with one or more of the data-type User Security Access Controls. 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.

To obtain access to any of this data, individual users submit a request to AFI through their User Access Manager, who then determines and approves the user security access controls based on the employee's need-to-know in the normal performance of official duties. A link description of these access controls is provided to users and User Access Managers during any provisioning process within AFI. Full definitions for all User Security Access Controls are listed in Appendix A.

User Access

In addition to existing user access controls, CBP updated the AFI Roles Summary document for User Access Managers' use that describes the search and access functions of the Consumer, Analyst, and Researcher roles defined above. The updated roles document provides increased guidance to supervisors on how to determine the correct roles for their employees and thus limits the risk that new users will be given unauthorized access privileges in AFI. A link description of the AFI Roles is provided to users and User Access Managers during any provisioning process within AFI.

[10] CBP restricts access to information in AFI based on user roles and role-based access determined by (1) a user's TECS profile for all source systems that reside on the TECS platform and (2) additional authorization if the source dataset does not reside on the TECS platform.
[11] Underlying source system data is not tagged by data type prior to indexing in AFI.

CBP approves new users and their access to AFI in two different procedures: (1) access to AFI search and analysis functionality and (2) access to the underlying data sources within AFI.

(1) Access to AFI Search and Analysis Functionalities
When setting up a new user account, CBP grants access to the different functionalities within AFI based on 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 profile. 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.

(2) Access to Underlying Data Sources via AFI Search and Analysis Tools
When a user requests access to AFI, he or she must select a User Access Role (i.e., Consumer, Analyst, or Researcher) and all applicable user security access controls (e.g., For Official Use Only (FOUO) or Passenger Name Record (PNR)), which will grant a user the ability to access underlying source data within AFI, as appropriate. 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 has selected the correct user security access controls. Supervisors are responsible for determining a new user's role based on the user's current position, clearance level, and need-to-know.

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 Requests for Information (RFI), as described in the 2012 PIA.

Review: The DHS Privacy Office received a demonstration of how potential users from pre-approved Components request access to AFI and how User Access Managers and AFI Administrators review the applications and approve or deny access. We reviewed the January 2015 AFI *User Administration Guide*, which includes instructions to apply for and approve access and defines User Role responsibilities and User Security Access Controls. We reviewed the CBP intranet AFI site, which includes useful information on accessing and using the system, as well as links to lists of User Access Managers. CBP also provided responses to questions detailing credential verification, user roles, user statistics, and user re-certifications.

We received a demonstration of the user log-in process, a briefing from CBP's Office of Information Technology (OIT) on the user credential verification application process at DHS, a demonstration of the steps a User Access Manager takes to review and approve/deny a new user request, and reviewed all product marking options. We were provided a demonstration of the search capability within AFI to verify whether search results matched the product markings.

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 OIT about the indexing tool.

Findings: At the time of the 2016 PCR, CBP was updating the AFI PIA to include a description of the Researcher role and an analysis of the expanded AFI user base that now includes ICE and USCIS users with a small number of users from I&A, TSA, and USCG. Before additional users can be added, AFI will complete a PTA documenting the new user group as well as use cases demonstrating why AFI access is necessary.

As of February 9, 2016, there were 2,444 users of AFI, down from 5,446 during the last PCR. This is a significant drop in AFI users, which may be attributed to more careful review by User Access Managers and the annual recertification process (discussed below). During the course of the PCR, AFI provided statistics that showed approximately 36 percent of user requests were denied due to the User Access Manager not having oversight of the user, demonstrating that these Managers will not verify a user request if they do not know the user and his or her job responsibilities directly. Additionally, access to individual data sources is determined by the source systems, meaning that if a user cannot be confirmed as having access to a particular source, the user is by default denied access within AFI. This is accomplished by a technical process that allows AFI to ask for and receive user permissions from another system to verify user privileges within the source system when users log in to AFI.

User Access Managers, with input from supervisors if necessary, annually review employee access to AFI data-types to ensure that users still require their given level of access. User Access Managers also must annually recertify their continued need to access AFI, which must be approved by another User Access Manager or AFI Administrator. Technical controls disable a user's account unless a User Access Manager and AFI Administrator both take action each year to re-authorize continued access for that user. Notification is provided to both the user and the User Access Manager who provided the last authorization for the user's account. If the recertification is not completed, then the user is automatically placed in a suspended mode and cannot access AFI. Additional controls require that access to data sources are governed by the source system (i.e., the user must already have access to the source system before having access to AFI products created from source system data). The *User Administration Guide* includes an update of the Roles Summary document and includes a description of user security access controls to assist the Manager in assigning appropriate roles.

The authorized users are almost equally divided between personnel from ICE and CBP, with a small number of users from I&A and USCIS (offices within TSA and USCG received approval to access AFI, but there were no active TSA or USCG users at the time of this review). The AFI program office had denied access requests from other DHS Components until the appropriate oversight mechanisms (discussed below) were in place to ensure mission compatibility with CBP.

The January 2015 AFI *User Administration Guide* provides supervisors with guidance in approving User Access and User Access Security Control settings. While the Guide is comprehensive and useful, several items appear outdated. The Guide should also be easily and readily accessible to the Manager within the system while in the process of approving or denying access. We were shown how a Manager processes a new user request, and found the Manager's vetting responsibilities and the ratio of managers and administrators to users to be reasonable. The AFI intranet site also includes useful information, but many links are not working, such as those regarding training, or information is outdated. It is unclear if the list of User Access Managers is current.

Recommendation 1: When User Access Managers and AFI Administrators seek annual AFI access recertification, Managers and Administrators should receive a copy of and affirm their awareness of their responsibilities within the *AFI User Administration Guide*.

Recommendation 2: Recognizing that CBP is drafting a comprehensive intelligence products SORN that will identify AFI's purpose, the individuals and records covered in AFI, and AFI's routine uses, this SORN should be finalized by the end of Fiscal Year 2017. The intelligence product SORN should also reflect changes in user roles, categories of individuals covered by the system, categories of records in the system, routine uses of records maintained in the system, and the data retention schedule.

C. Transparency

Requirement: The DHS Transparency FIPP states that DHS should provide notice to an individual when it collects, uses, disseminates, and maintains that person's PII. The AFI PIAs and SORN[12] have been posted to the DHS website since 2012, and the PCR[13] report was completed and posted in 2014. DHS Privacy Office Annual Reports[14] and DHS Data Mining Reports[15] have addressed AFI since the program's inception. Additionally, the DHS Office of the Inspector General (OIG) published its findings on technical controls to improve AFI's security in a September 2015 report.

Pursuant to the Privacy Act, agencies are required to provide what is commonly referred to as a Privacy Act or (e)(3) Statement to all persons asked to provide personal information about themselves, which will go into a system of records. While AFI does not directly collect personally identifiable information from individuals, the source systems from which AFI takes information include Privacy Act Statements at the point of collection. These statements provide notice regarding the authority to collect the information, uses of the information as described in the respective SORNs, and the consequences if the individual does not consent to providing the information.

[12] https://www.dhs.gov/publication/analytical-framework-intelligence-afi.
[13] https://www.dhs.gov/publication/privacy-compliance-review-analytical-framework-intelligence.
[14] https://www.dhs.gov/publication/privacy-office-annual-reports.
[15] https://www.dhs.gov/publication/dhs-data-mining-reports.

Review: We reviewed publically available documents that describe and discuss the privacy impact of AFI.

Findings: Although the AFI PIA was under revision during the course of our review, the new PIA was posted to the DHS website once finalized and we find that the program provides a number of other publically available options to meet the requirements of the Transparency FIPP.

D. Individual Participation

Requirement: The DHS Individual Participation FIPP states that when possible, DHS should 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.

Access Requests

Privacy Act and Freedom of Information Act (FOIA) requests are processed through the source system in which the personal information is held. To the extent that a record is exempted in a source system from being released, the exemption will continue to apply within AFI. To the extent there is no exemption for giving access to a record under the source system, the AFI SORN states that CBP will provide access to the information maintained in AFI. When an access 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 any applicable exemption, in accordance with procedures and points of contact published in the applicable SORN.

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 PIA for those systems. AFI refreshes the data from most source systems on at least a daily basis (many systems refresh on an hourly basis). 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. If incorrect information is discovered, a revised product is published to correct the information or note the questionable fact or content, and the incorrect product is removed from AFI. For any products that were externally disseminated and needing recall or correction, a recall message or revised product is disseminated to the recipients of the original product(s) with appropriate instructions. Individuals seeking notification of and access to any record contained in AFI, or seeking to contest its content, may submit a FOIA or Privacy Act request in writing to CBP. Additionally, 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 FOIA[16] or Privacy Act requests, and all responses, for information within the AFI System of Records. We discussed the process to respond to FOIA and Privacy Act requests with disclosure officials, as well as the protocol to release AFI records not otherwise exempt.

Findings: During the time period covered by the PCR, there were five FOIA requests for AFI information. All but one could be considered Privacy Act requests (as either direct requests or authorized third party requests), but all were also processed as FOIA requests per DHS regulations. In four of the five FOIA requests, AFI Records were not specifically requested. Rather, the records requested were travel records with generic language seeking access to CBP records. In such cases, CBP disclosure professionals use AFI to conduct a search of the source systems to identify responsive records and determine what information should be released. There is now a query tool within AFI whereby CBP disclosure professionals can efficiently conduct searches to find responsive documents to FOIA requests. This capability allows for one search within AFI that searches all source systems. The FOIA Division of the CBP Privacy and Diversity Office continues to work with the AFI team to develop this search capability and to provide access to information maintained in AFI's source systems, as appropriate. Due to responses to the previously low number of FOIA and Privacy Act requests, we found that appropriate steps are being taken to provide access to disclosure officials and promote transparency through non-exempted releases of information.

E. Purpose Specification

Requirement: The DHS Purpose Specification FIPP 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 information is used consistent with the authorities under which it was collected, CBP created the AFI Working Group (AFIWG), a governance board comprised of CBP offices including individuals from the Office of Intelligence (OI), Office of Field Operations (OFO), Privacy and Diversity Office (PDO), Office of Chief Counsel (OCC), Office of Information Technology (OIT), and other CBP stakeholders. The AFIWG directs the development of new aspects of the AFI system, including the review and approval of new or changed uses of AFI, new or updated user types and roles, and new or expanded data sources available to AFI. To prevent mission creep and ensure information used by AFI is consistent with the purposes for which it was originally collected, AFIWG is charged with reviewing and approving all information sharing agreements, Memorandums of Understanding (MOU) for new uses of the information, and new access to AFI by organizations within DHS.

CBP initiated the governance process when it finalized the AFIWG charter in August 2015. The AFIWG held its first meeting in September 2015 to oversee the new user requests for AFI access

[16] 5 U.S.C. § 552.

from DHS components, the inclusion of new data sources in AFI, and an expansion of user roles within AFI. CBP states the AFIWG meets regularly to ensure proper governance and to brief interested stakeholders on developments in AFI.

The AFIWG is also responsible for affirmatively approving all external (non-CBP) users who request access to AFI. A "need-to-know" checklist is being developed to assist AFIWG members determine whether any person requesting access may be granted access to AFI. The current AFI on-boarding criteria for new external users includes (1) membership in the DHS IE and (2) approval by the AFIWG.

Review: We reviewed the August 2015 AFIWG Charter and were briefed by AFI program staff on the process for adding new data sources to AFI.

Findings: While the AFIWG Charter was finalized in August 2015, the Privacy Office finds that the AFIWG could do more to demonstrate it is implementing its stated responsibilities. The 2016 PIA noted that the AFIWG reconvened in July 2016 to mitigate the risk that new users may be granted access to AFI outside the scope of CBP's border security mission and approved data access roles for specific Component offices.

It is imperative that the AFIWG fully implement its responsibilities defined in its Charter. An effective level of governance is essential to prevent mission creep, ensure that information used by AFI is consistent with the purposes for which it was originally collected, and ensure user groups meet the strict criteria for authorized access. The AFIWG may also be the appropriate means to oversee implementation of recommendations from this and the 2014 PCR.

> *Recommendation 3:* CBP should conduct regular AFIWG meetings and fully implement the governance structure, responsibilities, and procedures described in the AFIWG Charter.
>
> *Recommendation 4:* The AFIWG should monitor and report on implementation of all PCR recommendations and provide regular updates to the DHS Privacy Office with documentation showing corrective actions are completed.

F. Data Minimization

Requirement: The DHS Data Minimization FIPP 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 it is necessary to fulfill the specified purpose(s) of all programs.

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. Source data contained in AFI that has not been incorporated into a finished intelligence product or project follows the retention schedule set forth in the applicable source data SORN.

The Privacy Office will notify the DHS Records Management Office that it must complete National Archives and Records Administration (NARA) requirements to obtain a retention schedule across the Department for law enforcement intelligence products, including AFI products. As noted in the 2014 PCR, however, a finalized records retention schedule that includes AFI's finished intelligence products is still not completed. While the current retention and disposal language in the AFI SORN parallels the record schedules presently in place for similar records within the Department, CBP must work with the DHS Records Management Office to ensure timely completion.

Review: To assess compliance with the data minimization requirements, we reviewed PCR questionnaire responses, met with CBP disclosure officials, and received a demonstration of the indexing and recertification capabilities.

Findings: CBP has not completed a retention schedule for AFI, but is preparing a set of schedules to align with overarching DHS schedules for similar systems.

> *Recommendation 5:* CBP must work with the DHS Records Management Office to complete a records retention schedule for law enforcement intelligence products.

G. Data Quality and Integrity

Requirements: The DHS Data Quality and Integrity FIPP requires DHS to, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete. The 2012 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.

The 2016 PIA update notes that AFI now uses an open-source indexing tool to facilitate faster searches across multiple datasets, but that requires the system to store multiple copies of source data posing privacy concerns based on the continuous replication of data. To mitigate this privacy risk, AFI employs technical controls including checks that verify the data sent from source systems is the same data received by AFI and system awareness that can identify where the data being accessed by AFI is held. These technical controls preserve the integrity of the data being accessed by AFI by ensuring that the replicated copies of source system data are handled in same manner at the same time.

During the review, we received a briefing to discuss the open-source indexing tool that allows faster search across multiple datasets, but requires AFI to store multiple copies of all source data in multiple locations. While we believe duplicating information continues to pose a privacy risk, we found, and the 2016 PIA update confirms, that the vast majority of AFI source systems refresh at least daily. When data is modified or deleted in the source system, the technology ensures that the replicated copies reflect these changes in AFI, mitigating concerns that inaccurate or outdated data are being used for analytical purposes.

The vast majority of source data systems in AFI refresh at least daily and the program continues to improve the refresh rates of the data. The 2016 PIA notes that the source refresh rate depends on the size of the data set to be indexed, and the level of risk posed by data. While there remains a privacy risk that information within AFI will be inaccurate until the source systems refresh, technical controls manage replicated copies of source system data so that when data is modified or deleted, replicated copies are handled the same way at the same time. Additionally, the date of last refresh is communicated to users so they can determine if the information is timely enough. Users may then search the source system for the most current information. Lastly, CBP noted that because AFI is used to create analytical products with a longer-term lifecycle, the privacy risk of inaccurate data occurring with a daily refresh rate is more easily mitigated than if a product impacts a real-time situation.

Recertification

During the product development and publishing processes, there is an option to indicate whether the product contains PII. If PII is indicated, the product is flagged for annual PII recertification, which requires that users recertify any information marked as containing PII to ensure its continued relevance and accuracy. The publisher and his/her manager then receives an email annually to recertify if the product still contains PII. The email includes the project name, project owner, project creation date, last PII review date, and due date for current PII review. While the email is an effective timely reminder that PII recertification is required, the process to recertify should be better explained to project owners.

Analyst Workspace Collaboration

DHS AFI Analysts are responsible for the integrity of the products they create. Should an Analyst uncover erroneous information, he or she is required to correct the entry within AFI immediately upon determining it to be incorrect. This requirement also applies to any data to which an Analyst has access. Analysts are required by policy to make changes to the data records in the underlying DHS system of records if they identify inaccurate data, and alert the source system owner of the inaccuracy. AFI will then reflect the corrected information during source system refreshes. 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 to be recalled or corrected, a recall message or revised product will be disseminated to the recipients of the original product(s), or those that tagged the product with appropriate instructions for updating.

Also, a notification process exists in AFI to alert users when information in a product has been superseded by a new product.

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 with the authority to publish an approved Intelligence Product, which also allows users to edit product metadata and un-publish (retract) published products.

Review: Between AFI's inception and February 17, 2016, 5,044 products were published in AFI. AFI audit log data does not differentiate between products that have been corrected or un-published and re-published. If a product publisher determines that a published product is 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. Subsequently, when a user deletes a project, it is deleted from AFI and can no longer be accessed.

We reviewed responses to the AFI questionnaire, interviewed representatives from OIT, and received a demonstration of how to un-publish an erroneous product.

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.

Recommendation 6: CBP should continue to work toward an hourly 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: While the annual recertification emails are timely, additional instructions should be added within these emails to explain to project owners what is required of them and memorialized in policy.

Recommendation 8: CBP should update training and policies to explain the un-publishing process, and why/when a product should be un-published.

H. Security

Requirements: The DHS Security FIPP 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.

As part of a National Institute of Standards and Technology (NIST) security categorization process, CBP determines the criticality and sensitivity of information that AFI processes and stores. This helps ensure that AFI security controls are commensurate with the potential adverse impact on CBP operations and assets if there is a loss of confidentiality, integrity, or availability

of the system. According to AFI's system security plan dated December 2014, AFI's confidentiality and integrity impact levels were both categorized as high, while its availability impact level was moderate. These impact levels are used to determine baseline security controls needed for the system.

AFI employs the following security measures:

- All AFI users must consent to monitoring upon log-in or they cannot use the system.
- Role-Based Access Control determines a user's authorization to use different functions, capabilities, and classifications of data within AFI.
- Discretionary Access Control 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 information.
- AFI is developed to Intelligence Community Protection Level 2+ standards to prevent unauthorized access to data, ensuring that isolation between users and data is maintained based on a 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 Sensitive Systems Policy Directive 4300 A/B).

AFI's Authority to Operate expired in April 2016. On April 8, 2016, CBP OIT granted an Authority to Operate without following DHS policy, which does not consider the ATO valid if the privacy controls have not been adjudicated and the DHS Office of the Chief Information Security Officer (OCISO) Document Review approval has not been entered.

Review: We reviewed the OIG's September 2, 2015 report entitled, "Enhancements to Technical Controls Can Improve the Security of CBP's Analytical Framework for Intelligence,"[17] wherein CBP concurred with all recommendations and implemented corrective actions to address the OIG findings. We discussed the status of AFI's Authority to Operate with CBP and OCISO.

Findings: Pursuant to DHS Sensitive Systems Policy Directive 4300 A/B, systems may not receive an ATO without completed privacy compliance documentation, as approved by the DHS Chief Privacy Officer. CBP OIT revoked the unauthorized ATO once informed it did not adhere to DHS policy. CBP completed an updated Privacy Impact Assessment for AFI on September 1, 2016, and received a full Authority to Operate on September 9, 2016.

I. Accountability and Auditing

Requirements: The Accountability and Auditing FIPP holds DHS accountable for complying with the other privacy principles previously noted, providing training to all employees and

[17] https://www.oig.dhs.gov/assets/Mgmt/2015/OIG-15-137-Sep15.pdf.

contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

The 2012 PIA identifies AFI's extensive auditing procedures. The 2016 PIA confirms that AFI continues to enforce the same auditing and accountability policies, procedures, and practices identified in the 2012 PIA. Additionally, CBP has enhanced the auditing and accountability within AFI by creating and implementing the responsibilities of the AFIWG, which provides oversight of the system and provides a higher level of accountability. Furthermore, the addition of a new, open-source indexing tool prompted the addition of extra auditing and accountability processes specifically related to these functions.

AFI Search Results

AFI stores all user's search parameters, but not the search results themselves. AFI logs all search terms so that (1) users can re-run searches against new data in AFI following an underlying source data refresh and (2) auditors can ensure appropriate searches.

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. There were two notifications provided to the ISSO during the review period. One was suspected unauthorized access and the other was an unauthorized disclosure. Both instances were referred to and reviewed by Internal Affairs. AFI regularly reviews its automated security posture and monthly security scans revealed no additional suspicious events for the review period. AFI managers revoke a user's access when no longer needed or permitted. Technical controls monitor account/access retention that analyzes account creation, granting of access, and renewal dates for all users.

User Account Re-certifications and Audit

AFI enforces a user recertification process that requires User Access Managers to annually recertify all user permissions. Authorized users receive an annual email notice to recertify their need to access AFI and confirm that the appropriate User Security Access Controls match their current job functions. When a user completes the re-certification request, the request is routed to his or her User Access Manager for approval.[18] The system captures all of these actions in the user provisioning log. If the recertification is not completed, then the user is automatically placed in a suspended mode and cannot access AFI.

[18] The User Access Manager approves access to AFI only, and is not responsible for authorizing access to other data sources to which a user may or may not have access. A technical process allows AFI to ask for and receive user permissions from another system to verify user privileges within the source system when users log in to AFI. If a user cannot be confirmed as having access to a particular source, the user is by default denied access.

To keep an account active and maintain access to AFI, Users must access AFI at least once every 45 days. If more time elapses, the account is suspended, which requires action by the user and the designated AFI User Access Manager to reactivate. Users must also maintain an active TECS profile, which ensures the user has the required annual privacy training and the appropriate background investigation. AFI will automatically deactivate users who have their DHS Directory account locked or removed. This ensures that users who are terminated or otherwise disabled in the DHS network are likewise disabled in AFI.

User accounts without active access to AFI exist in one of three states: Archived (an AFI Administrator has removed them from the provisioning process), Inactive (accounts that belong to Users that requested access, but have not yet been approved for access by a User Access Manager and/or an AFI Administrator), and Suspended (accounts that belong to Users that have not logged in within 45 days or their User Access Manager has not approved the annual recertification). As of February, 22, 2016, there were 155 Archived accounts, 331 Inactive accounts, and 5,799 Suspended accounts. For auditing purposes, there is no process for complete removal of users from the system, even if their access is terminated. The AFI program determined that to audit a user's actions in the system for accountability purposes, 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.

In January 2015, the AFI program office updated guidance that includes a description of User Roles and User Security Access Controls to assist the User Access Manager in assigning appropriate roles. Additionally, User requests, supervisor approvals, and administrative actions are recorded in the User's profile. These procedures and updated internal guidance documents provide oversight and tracking of access controls assigned to individual users of AFI.

Finally, all AFI users are required to complete biannual training[19] in general privacy awareness as well as annual information security training, which include the appropriate uses and disclosures of the information they receive as part of their official duties as well as methods to safeguard the information in the system. Furthermore, AFI requires all users to have an active TECS profile and all users must complete annual recurring TECS-specific privacy training to maintain an active TECS profile. These trainings are regularly updated. Users who do not successfully complete these trainings will lose access to AFI.

Auditable Search Logs

AFI stores search terms and sources in auditable logs for all users, but not the search results. Audit logs also capture when users access Intelview documents. 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.

[19] This includes (1) annual TECS training and (2) annual DHS privacy training.

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 project page is logged as a change to the project. AFI noted that during the course of the PCR, a small number of users incorrectly requested the "security administrator role", which was promptly removed from their profile at the direction of the Information System Security Officer.

Review: To assess compliance with auditing and accountability controls within AFI, we 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 through automated technical controls, managerial, and AFIWG oversight. Implementing OIG recommendations has further strengthened AFI's oversight position.

IV. Conclusion

The DHS Privacy Office appreciates CBP's steps to ensure that AFI operates in a privacy-sensitive manner, as well as its 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 continued oversight and full implementation of PCR recommendations.

We discussed these eight recommendations with AFI program officials, CBP Privacy and Diversity Office staff, and the DHS Privacy Office Compliance Team, who are taking steps to implement them. The DHS Privacy Office requests a report from the AFIWG within six months from the publication of this PCR on the implementation status of the recommendations and regularly thereafter.

V. Privacy Compliance Review Approval

Responsible Official

Mario Medina
Director, Targeting Business Division
U.S. Customs and Border Protection

Approval Signature

Original signed copy on file with the DHS Privacy Office.

Jonathan R. Cantor
Acting 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 process. "User Security Access" impacts the products a user will be able to access in AFI IntelView and they will only be granted to said information in source systems for which they already have authorized access.

- AFI Users: Select the Security Access options for the types of data that they have a need to know in the normal performance of daily duties.
- AFI User Access Managers: Approve the Security Access options for the types of data that their 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, projects, RFIs and tasks that are identified as FOUO upon uploading into AFI (based on designation as FOUO or in the 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, projects, RFIs, and tasks that are identified as PCII upon uploading into AFI (based on PCII designation in the 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 C.F.R. 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, projects, RFIs and tasks that are identified as SSI upon uploading into AFI (based on SSI designation in the 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, projects, RFIs, and tasks that are identified as LES upon uploading into AFI (based on LES designation in the 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 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, projects, RFIs, and tasks that reference PNR upon uploading into AFI (based on PNR designation in the 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 that references PNR. PNR itself is not accessible in AFI and must be accessed in a separate CBP system.

Bank Secrecy
The United States' Bank Secrecy Act (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, projects, RFIs, and tasks that are identified as Bank Secrecy upon uploading into AFI (based on Bank Secrecy designation in the 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, projects, RFIs, and tasks that are identified as Trade Sensitive upon uploading into AFI (based on Trade Sensitive designation in the 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 United States persons in the product or information. 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 United States or are aliens lawfully admitted for permanent residence, or
- a corporation that is incorporated in the United States except for a corporation directed and controlled by a foreign government or governments.

Products, projects, RFIs, and tasks that are identified as U.S. Persons upon uploading into AFI (based on U.S. Persons designation in the 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.