Privacy Impact Assessment Update
for the

Analytical Framework for Intelligence (AFI)

DHS/CBP/PIA-010(a)

September 1, 2016

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

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The U.S. Customs and Border Protection's (CBP) Analytical Framework for Intelligence (AFI) system provides enhanced search and analytical capabilities to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and aids in the enforcement of customs, immigration, and other laws enforced by DHS at the border. Since the original Privacy Impact Assessment (PIA), CBP has increased technical safeguards in AFI; added a new user role, additional DHS users, and additional data sources; and developed a governance process that includes the operational and oversight components of CBP. CBP is updating the original AFI PIA to address Privacy Compliance Review (PCR) recommendations[1] and to promote transparency regarding the new users, data sources, data access, and analytic functions of AFI.

Overview

The U.S. Department of Homeland Security (DHS) published the original PIA for AFI in 2012.[2] CBP developed AFI to enhance CBP's ability to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and to improve border security. As part of CBP's authority to protect the border and enforce applicable laws at the border, CBP conducts research and analysis on its existing data systems to identify potential law enforcement or security risks and develop intelligence products. Prior to the deployment of AFI, analysts had to employ dozens of searches on individual data sources, and then manually read each search result for key elements such as names, dates, description of event, associates, and accomplices in a time-consuming process when conducting research and analysis. Analysts did not have a single access point to identify relevant data and use various tools to assist in the analysis and development of intelligence products.

The AFI system augments CBP's ability to gather and develop information about persons, events, and cargo or conveyances of interest by creating an index of the relevant data in the existing operational systems, and providing certain AFI users with different tools that assist in identifying non-obvious relationships. AFI allows certain users to research or publish tactical, operational, and strategic law enforcement intelligence products (hereinafter referred to as "finished intelligence products"). Finished intelligence products identify individuals or cargo (or conveyances) of greater security interest based on the targeting and derogatory information identified in or through CBP's

[1] Privacy Compliance Review for the Analytical Framework for Intelligence (December 19, 2014), *available at* https://www.dhs.gov/sites/default/files/publications/dhs-privacy-pcr-afi-12-19-2014.pdf.
[2] For a detailed description of the AFI system, please see DHS/CBP/PIA-010 Analytical Framework for Intelligence (AFI) (June 1, 2012), *available at* https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_afi_june_2012_0.pdf.

existing data systems. CBP currently uses transaction-based systems such as CBP TECS[3] (not an acronym) or the Automated Commercial Environment (ACE)[4] and the Automated Targeting System (ATS)[5] for targeting and inspections. AFI consolidates and enhances the information from those systems by using different analytical capabilities and tools that provide link analysis between data elements as well as the ability to detect trends, patterns, and emerging threats.

AFI Analytic Capabilities

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

AFI Search Functionality and Original Data Sources

In order to enable faster returns of search results, AFI creates an index of the relevant data in existing operational DHS source systems by ingesting this data from source data systems. The indexing engines refresh data from the originating system routinely depending on the source data system. Following the 2014 Privacy Compliance Review (PCR), the DHS Privacy Office recommended that CBP continue to work towards a one-to-one refresh rate for all underlying systems to minimize the potential for discrepancies between the data in AFI and the source systems. In response, CBP has achieved a latency of less than one hour for several data sources, and nearly all underlying systems are refreshed in real, or near-real time.[6]

When the AFI PIA was initially published in 2012, AFI used a proprietary search platform. AFI now uses a new, open-source platform that allows a much faster search across multiple datasets, but requires AFI to store multiple copies of all source data within the database platform. This platform 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 AFI, it presents privacy challenges as

[3] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing PIA, December 22, 2010, DHS/CBP/PIA-021 TECS Platform PIA, August 15, 2016, and DHS/CBP-011 U.S. Customs and Border Protection TECS SORN, December 19, 2008, 73 FR 77778, *available at* www.dhs.gov/privacy.
[4] *See* DHS/CBP/PIA-003 Automated Commercial Environment (ACE), July 31, 2015, and DHS/CBP-001 Import Information System, August 17, 2015, 80 FR 49256, *available at* www.dhs.gov/privacy.
[5] *See* DHS/CBP/PIA-006 Automated Targeting System PIA and subsequent updates, *available at* https://www.dhs.gov/publication/automated-targeting-system-ats-update.
[6] AFI refresh rates vary by data source; most are refreshed within 24 hours.

its functionality relies on continuous replication of data. This PIA update examines the privacy risks and mitigations associated with the new platform below.

AFI analysts and researchers are able to perform searches with more efficacy in AFI because the data has been indexed in a way that allows searches across all information in a record. Within AFI, this is a quick search that shows where a particular individual or data element arises. With other systems, a similar search for a particular individual requires several queries across multiple systems to retrieve a corresponding response.

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

- Automated Targeting System (ATS);[7]
- Advance Passenger Information System (APIS);[8]
- Electronic System for Travel Authorization (ESTA);[9]
- Border Crossing Information (BCI);[10]
- TECS;[11]
- Nonimmigrant and Immigrant Information System (NIIS);[12]
- Seized Asset Case Tracking System (SEACATS);[13]
- Department of Justice (DOJ) Federal Bureau of Investigation (FBI) Terrorist Screening Database;[14]
- Enterprise Management Information System-Enterprise Data Warehouse (EMIS-EDW), including:
    - Arrival and Departure Form (I-94);[15]
    - Currency or Monetary Instruments Report (CMIR) obtained from TECS;[16]
    - Apprehension information and National Security Entry-Exit Program (NSEERS) information from ENFORCE;[17] and

[7] *See* DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297.
[8] *See* DHS/CBP-005 Advance Passenger Information System (APIS), March 13, 2015, 80 FR 13407.
[9] *See* DHS/CBP-009 Electronic System for Travel Authorization (ESTA), February 23, 2016, 81 FR 8979.
[10] *See* DHS/CBP-007 Border Crossing Information (BCI), January 25, 2016, 81 FR 4040.
[11] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, December 19, 2008, 73 FR 77778.
[12] *See* DHS/CBP-016 Nonimmigrant and Immigrant Information System (NIIS), March 13, 2015, 80 FR 13398.
[13] *See* DHS/CBP-013 Seized Assets and Case Tracking System, December 19, 2008, 73 FR 77764.
[14] *See* DHS/ALL-030 Use of the Terrorist Screening Database System of Records, April 6, 2016, 81 FR 19988.
[15] *See* DHS/CBP-021 Arrival and Departure Information System (ADIS), November 18, 2015, 80 FR 72081.
[16] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, December 19, 2008, 73 FR 77778.
[17] *See* DHS/ICE-011 Immigration and Enforcement Operational Records (ENFORCE) System, April 30, 2015, 80 FR 24269. Additional information regarding NSEERS is available in DHS/CBP/PIA-006 Automated Targeting

- Student and Exchange Visitor Information System (SEVIS) information.[18]

Additionally, AFI permits certain AFI users to upload and store information that may be relevant from other sources, such as the Internet (including social media) or traditional news media, into projects or final intelligence products.[19] Finished intelligence products, and unfinished projects will also be searched when AFI users conduct analysis.

AFI improves the efficiency and effectiveness of CBP's research and analysis process by providing a platform for the research, collaboration, approval, and publication of finished intelligence products. AFI analysts and the newly added "researcher" role, described below, use AFI to conduct research on individuals and cargo to identify potential law enforcement or security risks.

Reason for the PIA Update

DHS/CBP is updating this PIA to conduct a privacy risk assessment of several changes and updates to AFI since the original PIA in 2012, including: (a) clarification and expansion regarding the procedures for AFI access; (b) procedures for approving non-CBP users; (c) addition of new data sources; and (d) CBP responses to several of the PCR recommendations.

A. Procedures for AFI Access

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 (see below for detailed discussion of the TECS profile and how it is used to determine access to the underlying data

System (ATS) PIA and subsequent updates, and DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297, *available at* www.dhs.gov/privacy.

[18] *See* DHS/ICE-001 Student and Exchange Visitor Information System (SEVIS), January 5, 2010, 75 FR 412.

[19] *See* DHS/CBP-017 Analytical Framework for Intelligence System, June 7, 2012, 77 FR 13813, which "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."

sources as well) and has completed the appropriate training. 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.

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.

The original AFI PIA describes the AFI Analyst and Finished Intelligence Product User roles (now referred to as the "Consumer" role), however since publication of the PIA, the AFI program has updated its user provisioning to include three distinct user access roles. This PIA update provides additional clarity regarding the data access and user functionality of each role.

- Consumer – Consumers are DHS personnel referred to as the "finished intelligence product users" in the 2012 AFI PIA, and 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 is the minimum role for all AFI users.

- Researchers – Researchers perform complex data searches across any data source to which they have access. 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. If a Researcher does not have access to information in a source system, results from that system will not populate an analyst's search results in AFI.

- Analyst – All Analysts have the Researcher role. 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.

Researchers use AFI to obtain a more comprehensive view of data available to CBP, and then analyze and interpret the data using the visualization[20] and collaboration tools accessible in AFI. Consumers on the other hand have more limited access to AFI and only view the finished tactical, operational, and strategic intelligence products published in AFI. Consumers do not have access to the AFI data underlying those products. Only Researchers have access to the analytical tools.[21] Researchers use the data from AFI source systems either in the analytical tool or in the AFI project space where collaboration with other designated users of the information may occur. Finally, the Analyst role is functionally equivalent to the Researcher role, with the exception that Analysts are reserved for CBP AFI users who require specific tool usage. Currently, AFI is not using any CBP-specific tools.

User Functionality Roles

In addition to the three user roles defined above, AFI users may have other functional roles to perform their job functions within the system. The three roles above correspond to what types of information *a user can search*. The following functional roles correspond to information that a user *can create*. For example, a Consumer is only able to view finished intelligence products and cannot search underlying source information. However, based on information already available to them as part of their job duties (regardless of AFI access), a Consumer may still be able to author or publish finished intelligence products of relevance to their job function. An operational Consumer with the author/publication role may be a CBP Agricultural Specialist who does not require access to underlying PII-heavy datasets, but would still author, publish, and share intelligence products related to pests and agricultural threats.

The functional roles supported by AFI are:

- Product Author – this role allows users to create, edit, and submit finished intelligence products for review and eventual dissemination within the AFI IntelView library;
- Product Manager – this role allows users to approve finished intelligence products for publication in the IntelView library. All users with the Product Manager role will also have the Product Author role;
- Product Publisher – this role allows users to publish or remove finished intelligence products in AFI.

[20] Visualization tools present data in graphic or other pictorial form to allow analysts to see relationships among data.
[21] Analytical tools allow analysts to perform statistical or other mathematical operations to identify relationships among data.

- Executive Statistics – this role allows users to view AFI usage reports and statistics. Only users with system management responsibilities are approved for this role;
- User Access Manager – Users with this role can approve or reject user access changes and annual access certifications. Access Managers are responsible for ensuring that user access requests in AFI are commensurate with their job functions. Access Mangers are also responsible for maintaining (National Data Exchange (N-DEx)[22] training certificates for users requesting access to Law Enforcement Information Sharing Service (LEISS) data sources;
- User Admin – User Administrators provide second-level approval to complete user provisioning for new users requesting access to AFI;
- Law Enforcement Technical Collections (LETC) Reports – this role enables users to access LETC's reporting capability. Approved users can run and view reports to analyze LETC data but they cannot view or edit the raw LETC data. AFI restricts this role to only CBP users who have been approved by the Office of Intelligence (OI) to view LETC reports; and
- LEISS – this role enables AFI users the ability to access and use information obtained via the LEISS data sources for official law enforcement, criminal justice, or national security purposes only. As mentioned above, in addition to a valid TECS profile, all users with the LEISS role must supply their Originating Agency Identifier (ORI) Code[23] and have a valid N-DEx training certificate from the FBI.

Researchers and Analysts have access to raw data obtained from the underlying source systems, analytical tools, and have the ability to create projects and law enforcement intelligence products. Consumers on the other hand, only have access to finished intelligence products published to the AFI IntelView and will not have access to raw data or analytical tools. However, any Consumer that also is approved for the Product Publisher role will have the ability to publish finished intelligence products within AFI.

(2) Access to the underlying data sources within AFI

CBP restricts access to information in AFI based on user roles (described above), and role-based access determined by (1) a user's TECS profile for all source systems that reside on the

[22] N-DEx provides criminal justice agencies with an online tool for sharing, searching, linking, and analyzing information across jurisdictional boundaries. N-DEx training required to access LEISS.
[23] An Originating Agency Identifier (ORI) Code is a unique identifier assigned by the FBI to all law enforcement agencies who wish to access DOJ and FBI law enforcement information sharing services.

TECS platform,[24] and (2) additional authorization if the source dataset does not reside on the TECS platform.

Systems that reside on the TECS Platform

All AFI users must have an active TECS account. In order to gain and maintain access to TECS information, a user must have, at a minimum, the appropriate background investigation and successfully take and pass the annual TECS Security and Privacy Awareness course, as well as have a need to know TECS information. Every new and existing user of TECS is assigned a System Control Officer (SCO) who is responsible for the user's profile record and assigns the role(s) and the functions within that role. TECS user accounts are reviewed periodically and certified annually to ensure that these standards are maintained.

All AFI user accounts are mapped to the individual user's TECS profile. Therefore, the TECS profile controls access to all underlying datasets within AFI that reside on the TECS platform or use the TECS profile to controls access. Relying on the TECS profile to determine access to the underlying sources in AFI ensures that no AFI users can access any TECS data sources within AFI that they would not be able to otherwise access in TECS. All user access to source data in AFI matches the same datasets they can access in TECS, determined by roles and functions assigned to an individual's TECS profile pursuant to their need-to-know to perform their official job duties.

The underlying data sources that can be viewed in AFI with only an active TECS profile are:

- Finished intelligence products in AFI IntelView;
- AFI projects;[25]
- ICE NameTrace data from the ICE Intelligence Reporting System (IRS);
- APIS records;
- CMIRs records;
- I-94 arrival and departure records;[26]
- Primary person and vehicle border crossing information;
- Records of passengers who are referred to secondary inspection;

[24] DHS/CBP/PIA-021 TECS Platform, *available at* www.dhs.gov/privacy.
[25] 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.
[26] *See* DHS/CBP-021 Arrival and Departure Information System (ADIS), November 18, 2015, 80 FR 72081.

- TECS incident log reports;
- Arrest and seizure incident reports from SEACATS;
- Visa applicant records;
- Watchlist Service records;
- Intelligence information derived from Detention and Removal Officers (DRO);
- CBP Field Information Reports (FIR) and Homeland Security Intelligence Reports (HSIR) from the IRS; and
- Commercial data aggregator records.

Datasets that do not reside on the TECS Platform

Within AFI, there are other data sources that require additional authorizations as well as an active TECS profile to access the data in AFI. For example, some records require the TECS profile plus an ORI code[27] that confirms an individual belongs to the organization approved to view that particular data source in AFI. The data sources that require additional requirements for access in AFI are:

- ICE Enforcement Integrated Database (EID)[28] records;
- ICE intelligence products (includes finished intelligence products, HSIRs, Homeland Security Assessments (HSA), and intelligence notes);
- TECS Reports of Investigation (ROI);
- Information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department;
- Shipment data related to specific trade records;[29]
- Electronic System for Travel Authorization (ESTA) records;
- National Security Entry Exit Registration System (NSEERS) records;

[27] An Originating Agency Identifier (ORI) Code is a unique identifier assigned by the FBI to all law enforcement agencies that wish to access DOJ and FBI law enforcement information sharing services.
[28] For a detailed description of the EID system, please see DHS/ICE/PIA-015 Enforcement Integrated Database (EID) (April 8, 2014), *available at https://www.dhs.gov/publication/dhs-ice-pia-015-f-enforcement-integrated-database.*
[29] This refers to entry summary data sourced from the Automated Commercial Service (ACS). When ACS is retired, entry summary data will need to be sourced from ACE. *See* DHS/CBP/PIA-003 Automated Commercial Environment (ACE), July 31, 2015, *available at* https://www.dhs.gov/publication/filing-data-acsace.

- Student and Exchange Visitor Information System (SEVIS) records; and
- LEISS records.

B. Procedures for Approving Non-CBP Users

In 2012, CBP's Office of Intelligence and Investigative Liaison (OIIL) (now known as the Office of Intelligence) developed AFI to enhance CBP's ability to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and to improve border security. The initial deployment of AFI was limited to CBP users, including OIIL analysts, Border Patrol Agents, Air and Marine Officers, Office of Field Operations (OFO) Officers, and Office of Information Technology (OIT) specialists. Following the initial deployment of AFI, CBP has added new users from across the CBP organization, since AFI was originally developed and intended to be used to improve and enhance any and all CBP mission functionalities. For example, the CBP Privacy and Diversity Office (PDO), Freedom of Information Act (FOIA) Division has access to AFI to conduct their TECS searches for faster and more efficient results.

While AFI was developed primarily to be used in support of CBP's border security mission, and therefore available to all CBP users with a need to know, AFI has expanded to allow access for members of the DHS Intelligence Enterprise[30] (IE), *with approval from* the AFI Working Group (AFIWG), AFI's governance and oversight mechanism discussed in detail below. The primary function of DHS IE is to coordinate and de-conflict the national and Departmental intelligence functions in support of DHS's intelligence mission. The DHS IE is organized through Component Intelligence Programs (CIP) and includes any organization within a DHS component that collects, processes, analyses, produces, or disseminates intelligence, regardless of the substance of the information. Moreover, any DHS component that employs intelligence professionals to perform intelligence functions is considered a CIP and therefore considered a member of the DHS IE.

All approved non-CBP users who have been granted access to AFI, with approval of the AFIWG, are included in an Appendix to this PIA update. This Appendix will be updated as new users are approved.

C. New AFI Source Datasets

In addition to responding to the AFI PCR recommendations, DHS/CBP is updating this PIA to document additional data sources within AFI since the last PIA was published in 2012.

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

Since then, AFI has added both ICE and local law enforcement data sources. In addition to the data sources listed in the previous PIA, AFI now ingests the following data sources from ICE:

- Enforcement Integrated Database detention data;
- ENFORCE Alien Removal Module;
- ENFORCE Alien Detention Module;
- ICE intelligence information reports;
- ICE intelligence products;
- ICE Name Trace; and
- Significant Event Notification Detention and Removal Office leads.

Ingesting these new ICE data sources provides analysts and researchers with more information to generate finished intelligence products that better informs DHS employees and provides context for the targeting and derogatory information identified in underlying source systems. The new ICE data sources will allow Analysts and Researchers to identify individuals, associations, relationships, or patterns that may pose a potential law enforcement or security risk, target cargo that may present a threat, and assist finished intelligence product users in the field in preventing the illegal entry of people or goods, or identifying other violations of law or regulations at and/or between ports of entry.

In addition to the new ICE data sources, AFI now provides access to the Law Enforcement Information Sharing Services (LEISS) data sources which include:

- The Automated Regional Justice Information System;[31]
- Central Arizona, Phoenix Police Department Person Search;
- East Arizona, Mesa Police Department Person Search;
- North Arizona, Maricopa County Police Department Person Search;
- South Arizona, Tucson Police Department Person Search;
- Los Angeles Police Department Person Search;
- Law Enforcement Information Exchange –National Capital Region;
- Law Enforcement Information Exchange –Hampton Roads, VA;
- Law Enforcement Information Exchange –California; and

[31] The Automated Regional Justice Information System (ARJIS) was created to share information among justice agencies throughout San Diego and Imperial Counties, California. For additional information, please *see* http://www.arjis.org/SitePages/WhatIsARJIS.aspx.

- FBI National Data Exchange System.[32]

The LEISS data sources allow approved Researchers to access state and local criminal repositories for law enforcement, criminal justice, or national security purposes. These LEISS data sources will not be ingested by AFI, rather AFI will act as a portal for authorized users to access the LEISS information. Previously, ICE analysts utilized the Authoritative ICE Data Warehouse (AIDW) system to access LEISS data; however, by leveraging AFI as a portal, ICE was able to deactivate AIDW thereby saving DHS significant resources. All authorized Researchers can access LEISS data in AFI though the external search tab provided they have an active TECS profile, have taken the requisite training, and are eligible to view LEISS data. Researchers will use LEISS data to cross-reference, confirm, and broaden the scope of information available within AFI about an individual of interest.

D. Privacy Compliance Review (PCR) Recommendations and Implementation

PCR Recommendation #1: Researcher Role and New Users

CBP has conducted a thorough update of the previously issued AFI PIA to describe the various user access roles. Please see the "Access to AFI Search and Analysis Functionalities" previously described in this document.

PCR Recommendation #5 and #10: Addition of Open-Source Platform

AFI now uses a new, open-source indexing tool that allows a much faster search across multiple datasets at a lower computational cost than the previous Oracle-based search platform. AFI users can now conduct larger searches across multiple datasets and at a quicker rate, promoting operational efficiency. To facilitate these faster searches, AFI now stores multiple copies of data in multiple machines/servers within the data center. The new indexing tool provides for shared storage and analysis by replicating the underlying data sources, and storing the replicated data in multiple machines/servers within the same data center to prevent system failure.

For a detailed description of the privacy risk and mitigation strategy employed by CBP, please see the "Uses of the Information" Privacy Impact Analysis subsection below.

Privacy Compliance Review Recommendation #9: AFI Working Group

The AFI Working Group (AFIWG), is a governance board comprised of CBP component offices including individuals from 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,

[32] *See* Privacy Impact Assessment for the National Data Exchange (N-DEx) System (May 9, 2014), *available at* https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/N-DEx; and FBI-020 Law Enforcement National Data Exchange System (NDEX) (October 4, 2007, 72 FR 56793).

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. The governance board also reviews and approves all information sharing agreements, Memorandums of Understanding (MOU) for new uses of the information, and new access to AFI by organizations within DHS thereby preventing mission creep and ensuring that information used by AFI is consistent with the purposes for which it was originally collected.

CBP implemented AFI PCR Recommendation #9 to reconvene the governance process and finalize the AFI charter. CBP reestablished the AFIWG in August 2015, and held the first meeting in September 2015, to oversee the new user requests for AFI access from DHS components, the inclusion of new data sources in AFI, and an expansion of user roles within AFI. The AFIWG continues to meet 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. At this time, the AFIWG on-boarding criteria for new external users includes (1) membership in the DHS IE and (2) approval by the AFIWG.

Privacy Compliance Review Recommendation #15: Data Labeling Correction

In addition to requesting user roles, potential users requesting access to AFI must also specify the data-types to which they require access. Upon creation of a product, a user must mark the product with one or more of the data-type security access controls. One of the data-types found within AFI is U.S. Person data and all products containing U.S. Person data must be appropriately tagged upon creation. This designation is used to identify products or information that would need additional review prior to release to elements of the Intelligence Community (IC), due to the inclusion of specific identifying characteristics of U.S. Persons in the product or information.

Privacy Impact Analysis

Authorities and Other Requirements

No change.

Characterization of the Information

The characterization of information has changed since the last PIA was published. In particular, AFI now includes more data from the newly added sources noted above, which could

lead to new leads on intelligence or law enforcement actions. Furthermore, the addition of the ICE and LEISS data sources enhances AFI's search and analytic capabilities and allows information to be used in new ways. There is, however, no change to how the AFI system disseminates or maintains information. Likewise, the primary purpose for the collection of this information remains the same, however, these minor changes do have the potential to modify the characterization of information due to the addition of new analytical tools combined with new information sources.

The data sources for AFI remain the same but also include new data sources from ICE and LEISS as discussed below. The information is still collected through source systems with AFI performing searches for and accessing information collected and maintained in these other systems. The AFI system acts as a repository for data sent to the system from other federal, state, and local law enforcement organizations. AFI does not collect any data directly from the public.

Privacy Risk: There is a risk that data collected from newly added sources could be used for purposes outside of the purpose for which the information was originally collected.

Mitigation: The AFI system enforces the access controls established by source systems – either by using the TECS profile controls or additional access controls (such as an agency ORI code for local law enforcement information). Users cannot gain access to information in AFI if they cannot access the information in the original source systems. Additionally, CBP mitigates this risk by carefully vetting the addition of any new data through the AFIWG. As the governance body for AFI, the AFIWG 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. Moreover, routine audits of system access ensure that analysts and researchers employ information consistent with the purposes for which it was collected. Furthermore, PCRs conducted by the DHS Privacy Office mitigate this risk by assessing CBP's success in managing risks related to the characterization of information.

Uses of the Information

The previous PIA discussed how the AFI system uses technology to conduct electronic searches, queries, or analysis in the system. As mentioned above, this PIA is being updated to note that AFI now uses an open-source indexing tool that facilitates faster searches across multiple datasets with lower maintenance costs, but requires the system to store multiple copies of source data and therefore poses significant privacy concerns based on the continuous replication of data. This PIA update also addressed the addition of new users from other DHS components as well as the inclusion of new data sources in the system.

As a result of these changes, CBP is updating this PIA to document the privacy risks concerning the changes to AFI as well as to provide transparency on the safeguards employed to appropriately mitigate those risks.

Privacy Risk: AFI does not track users by Component Office or mission; therefore, it is impossible to tell whether a user who has access to specific information within AFI has a job function that requires such access.

Mitigation: Following the initial deployment of AFI, CBP has added new users from across the CBP organization, since AFI was originally developed and intended to be used to improve and enhance any and all CBP mission functionalities. While AFI was developed primarily to be used in support of CBP's border security mission, and therefore available to all CBP users with a need to know, AFI has expanded to allow access for members of the DHS Intelligence Enterprise[33] (DHS IE), *with approval from* the AFI Working Group (AFIWG), AFI's governance and oversight mechanism discussed in detail above. The AFIWG is also responsible for affirmatively approving all external (non-CBP) users who request access to AFI.

At this time, the AFIWG on-boarding criteria for new external users includes (1) membership in the DHS IE and (2) approval by the AFIWG. All external users are listed in an Appendix to this PIA.

Privacy Risk: There is a risk of unauthorized access to AFI.

Mitigation: AFI enforces an annual user recertification requiring User Access Managers to annually recertify all user permissions. If the recertification is not completed, then the user is automatically placed in a suspended mode and cannot access AFI. In January 2015, the AFI program office updated user role documentation to now include a description of user security roles to assist the access manager in the assignment of appropriate roles. Additionally, user profile requests, supervisor approvals, and administrative actions are recorded in the profile. These procedures and updated internal guidance document ensure that there is sufficient oversight and tracking of appropriate security access controls assigned to individual users of AFI.

AFI also enforces an annual user recertification process that requires user access managers to annually recertify all user permissions. If the recertification is not completed, then the user is automatically placed in a suspended mode and cannot access AFI.

In addition to existing user access controls, CBP has updated the AFI Roles Summary document accessed by User Access Managers in AFI to describe in a narrative format the search and access functions of the Consumer, Analyst, and Researcher roles defined above. Previously, the AFI Role Summary document only included a description of each role's technical function in AFI. The updated roles document provides increased guidance to supervisors on how to determine

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

the correct roles for their employees and thus limits the risk that new users will be given unauthorized access privileges in AFI.

Unauthorized access is further mitigated by AFI's enforcement of the access controls established by source systems through the TECS profile or other additional access control measures (such as the agency ORI code, described above). 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 individuals authorized to access the data in the source system have access to that same data through AFI. This is accomplished by passing user credentials via the TECS profile or through additional access controls (such as an agency ORI code for local law enforcement information).

Moreover, AFI users with the Product Publisher functionality role must designate user security access controls for each intelligence product prior to publication so that it may be made available appropriately. Marking intelligence products prior to publication 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, the Product Publisher creates restrictions with respect to the group of finished intelligence product users who may view the product, thereby further limiting the risk that a user may obtain unauthorized access to data in AFI.

Finally, all AFI users are required to complete biannual training 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.

Privacy Risk: Under the previous Oracle-based search platform, AFI was able to index the underlying source system data without retaining a complete copy of the responsive data. With the deployment of the new indexing tool, AFI now stores multiple copies of all DHS source system data on multiple machines/servers, thereby improving the performance and integrity of the system. The storage of multiple copies of source data increases the risk that more data is held than what is needed in order for the system to provide accurate analysis. Because AFI uses a highly distributed file system (HDFS), which requires replication of data across multiple "nodes" and "clusters" to permit analytical tools to conduct queries across multiple datasets in real-time, there is an increased risk of unauthorized access to multiple copies of AFI and source data sets stored across multiple nodes and clusters.

Mitigation: The use of a new, open-source indexing tool to bolster the search and analytic capabilities of AFI has resulted in the replication of data sets within a new environment, which is principally designed to improve use of the data for analysis and dissemination. 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 which machine/server within the cluster holds the data being accessed by AFI. 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.

The privacy risk of inaccurate data posed by a continuous replication of data is further mitigated by new refresh rates for all data sources in AFI. AFI now refreshes most data sources at least daily, though many data sources refresh every few hours or on a real time basis. When data is modified or deleted in the source system, the technology ensures that the replicated copies reflect these changes in AFI.

Lastly, the nature of an HDFS security architecture is privacy enhancing by design. Data from AFI and the source data sets are distributed across multiple storage nodes and clusters, all with technical and security controls (including encryption) to prevent unauthorized access. This method of storage and retrieval is privacy-enhancing because nodes and clusters do not maintain an entire dataset, but rather pieces of data from the original data set. HDFS works in large, scalable environments in a secure manner by replicating large datasets across thousands of nodes and clusters, spread across servers in different geographic locations. If one node is compromised or fails, data is replicated into other nodes, but without proper security tokens authentication to the entire node or cluster, or front-end application (AFI), any data compromised from a single node would be unusable to an attacker.

Privacy Risk: There is a risk that information within AFI will be inaccurate until the source systems refresh. Despite the speed of AFI's search and analysis capabilities, the refresh rates for the underlying source systems are not instantaneous.

Mitigation: This risk is partially mitigated. The program continues to improve the refresh rates of the data. 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 United States has a faster refresh rate than trade entry information. To further mitigate this risk the date of last refresh is communicated to the users. This allows users to recognize when their search may require records for the most current events that would only be available in the source system. Users may then search the source system for the most current information.

Privacy Risk: There is a risk that individuals will not be able to correct erroneous information about themselves.

Mitigation: All Privacy Act or DHS Traveler Redress Inquiry Program (TRIP) requests for access, correction, or redress of records are conducted via the underlying source systems. AFI refreshes the data from most source systems on at least a daily basis (many systems refresh on an hourly basis) as noted above. Since AFI draws upon other source systems for its data, any changes

to source system records, or the addition or deletion of source system records, will be reflected in corresponding amendments to the AFI index as the index is periodically updated.

At times, it is possible that erroneous information may be published in a finished intelligence product. When incorrect information is discovered, a revised product will be published to correct the information or note the questionable fact or content, and the incorrect product will be removed from AFI. Misinterpretation or misstatement in an approved, published, intelligence report may be discovered through subsequent review and the feedback process. Through the addition of more consumers, reporting quality should improve. For any products that were externally disseminated and needing recall or correction, a recall message or revised product will be disseminated to the recipients of the original product(s) with appropriate instructions.

Privacy Risk: There is a risk that new users may be granted access to AFI outside the scope of CBP's border security mission.

Mitigation: The AFIWG reconvened in July 2016, and determined that the standards for approval will be based on either (1) CBP user or (2) membership in the DHS Intelligence Enterprise, *with approval of the AFIWG*. The AFIWG was satisfied that each of the offices listed in the Appendix could establish a sufficient "need-to-know" consistent with CBP's border security or DHS intelligence enterprise mission(s). The AFIWG approved both Consumer and Researcher data access roles for each of the new components gaining access to AFI.

Notice

No Change.

Data Retention by the project

No Change.

Information Sharing

No Change.

Redress

No Change.

Auditing and Accountability

AFI continues to enforce the same auditing and accountability policies, procedures, and practices identified in the previous PIA. However, 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 than discussed in the last PIA. Furthermore, the addition of a new, open-source indexing tool prompted the addition of extra auditing and accountability processes specifically related to these functions.

Responsible Official

Mario Medina
Director, Targeting Business Division
U.S. Customs and Border Protection
Department of Homeland Security

Debra L. Danisek
Acting CBP Privacy Officer
U.S. Customs and Border Protection
Department of Homeland Security

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: Approved AFI External Users

(non-CBP users)

While AFI was developed primarily to be used in support of CBP's border security mission, and therefore available to all CBP users with a need to know, AFI has expanded to allow access for members of the DHS Intelligence Enterprise[34] (DHS IE), *with approval from* the AFI Working Group (AFIWG), AFI's governance and oversight mechanism discussed in detail above. The primary function of DHS IE is to coordinate and de-conflict the national and Departmental intelligence functions in support of DHS's intelligence mission. The DHS IE is organized through Component Intelligence Programs (CIP) and includes any organization within a DHS component that collects, processes, analyses, produces or disseminates intelligence, regardless of the substance of the information. Moreover, any DHS component that employs intelligence professionals to perform intelligence functions is considered a CIP and therefore considered a member of the DHS IE.

All approved non-CBP users who have been granted access to AFI, with approval of the AFIWG, are included in an Appendix to this PIA update. This Appendix will be updated as new users are approved.

1. United States Citizenship and Immigration Services (USCIS): Fraud Detection and National Security Directorate (FDNS)

The FDNS leads USCIS's effort to ensure that immigration benefits are not granted to persons who pose a threat to national security or public safety. FDNS employees originally needed access to AFI because ICE decommissioned their Intelligence Fusion System (IFS). The IFS allowed FDNS employees to identify individuals who posed a potential security risk and aided in the enforcement of immigration laws. Access to AFI re-establishes FDNS's capability to assist with I-94 updates; to search multiple systems for indications of immigration fraud; to identify persons of national security or law enforcement interest; and to facilitate immigration fraud and benefit eligibility determinations.

2. Immigration Customs Enforcement (ICE): Homeland Security Investigations Office of Intelligence (including Intelligence personnel in Field Offices)

CBP has granted AFI user accounts to certain ICE personnel, including personnel from Homeland Security Investigations and Enforcement and Removal Operations for the purpose of facilitating law enforcement and law enforcement intelligence objectives, as well as the administration of immigration laws and other laws enforced by ICE. ICE is a critical investigative arm of DHS and is a vital U.S. asset in combating criminal organizations illegally exploiting the

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

United States' travel, trade, financial, and immigration systems. ICE has broad legal authority to investigate and enforce laws related to cross-border criminal activity including financial crimes, commercial fraud, cybercrimes, human smuggling and trafficking, immigration fraud, narcotics and weapons smuggling, and transnational gang activity.

3. Transportation Security Administration (TSA): Office of Intelligence & Analysis (Threat Analysis Division, Field Intelligence Division, and the Encounter Analysis Branch in the Vetting Analysis Division)

CBP has granted AFI user accounts to certain TSA personnel to aide in identity resolution and threat assessment of passengers matched to watch lists in the Secure Flight system and for transportation sector workers in TSA's credentialing process. CBP has also granted TSA users accounts for access to intelligence products contained in the system to perform transportation security functions. Products may be used to corroborate intelligence work, provide insight into other threat avenues, or provide different perspectives from different finished intelligence products.

4. United States Coast Guard (USCG): Office of Intelligence (CG-2)

USCG Intelligence Enterprise analysts access to AFI increases the ability of the USCG to identify all adversaries and threats enhancing maritime domain awareness, bolster indications and warnings, and help supply the DHS Intelligence Enterprise with all-source, integrated, finished intelligence. Access to AFI will also assist in the identification of individuals who pose potential security risks and aid in the enforcement of maritime law enforcement and regulatory authorities. The potential user base would consist of approximately 350 intelligence analysts located at the USCG Intelligence Coordination Center, USCG Counterintelligence Service, USCG Cyber Command, both Maritime Intelligence Fusion Centers, and several field intelligence units.

Additionally, USCG Intelligence is currently researching how to integrate its own wealth of law enforcement reporting (i.e. CG Field Intelligence Reports) into DHS systems, to include AFI. If CG Field Intelligence Reports are added as a source within AFI, this PIA and/or Appendix will be updated.

5. DHS Office of Intelligence and Analysis (I&A)

Users from DHS I&A have been granted access to AFI to assist in enhancing the understanding of and response to threats to aviation security, increasing operational effectiveness against threats to the security of the U.S. borders, and assisting in countering violent extremism. DHS I&A's mission is to equip the Homeland Security Enterprise with the intelligence and information it needs to keep the homeland safe, secure, and resilient. DHS I&A will use AFI to identify individuals, associations, or relationships that may pose a potential law enforcement or security risk. CBP granted AFI user accounts to certain DHS I&A personnel for the purpose of

facilitating the identification of individuals, associations, or relationships that may pose a potential law enforcement or security risk under the laws administered or enforced by DHS.