This document is scheduled to be published in the
Federal Register on 06/07/2012 and available online at
http://federalregister.gov/a/2012-13815, and on **FDsys.gov**

9110-06

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2011-0114]

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

AGENCY: Privacy Office, DHS.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security is giving concurrent notice of a newly established system of records pursuant to the Privacy Act of 1974 for the "Department of Homeland Security/U.S. Customs and Border Protection—017 Analytical Framework for Intelligence (AFI) System of Records" and this proposed rulemaking. In this proposed rulemaking, the Department proposes to exempt the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: Comments must be received on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2012-0114, by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

- Fax: 703-483-2999.
- Mail: Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

Instructions: All submissions received must include the agency name and docket number for this notice. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Laurence E. Castelli (202-325-0280), CBP Privacy Officer, Office of International Trade, U.S. Customs and Border Protection, Mint Annex, 799 Ninth Street, NW, Washington, D.C. 20229. For privacy issues please contact: Mary Ellen Callahan (703-235-0780), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background:

In accordance with the Privacy Act of 1974, 5 U.S.C. § 552a, the Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) proposes to establish a new DHS system of records titled, "DHS/ U.S. Customs and Border Protection, DHS/CBP—017 Analytical Framework for Intelligence (AFI) System of Records."

AFI enhances DHS's ability to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk; and aids in the enforcement of

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

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

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

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

Two principal types of users will access AFI: DHS analysts and DHS finished intelligence product users. Analysts will use the system to obtain a more comprehensive view of data available to CBP, and then analyze and interpret that data using the visualization and collaboration tools accessible in AFI. If an analyst finds actionable terrorist, law enforcement, or intelligence information, he may use relevant information to produce a report, create an alert, or take some other appropriate action within DHS's mission and authorities. In addition to using AFI as a workspace to analyze and interpret data, analysts may submit or respond to RFIs, assign tasks, or create finished intelligence products based on their research or in response to an RFI. Finished intelligence product users are officers, agents, and employees of DHS who have been determined to have a need to know in the performance of their official duties and who have appropriate clearances or permissions. Finished intelligence product users will have more limited access to AFI, will not have access to the research space or tools, and will only view

finished intelligence products that analysts published in AFI. Finished intelligence product users are not able to query the data from the source systems through AFI.

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

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

DHS is claiming exemptions from certain requirements of the Privacy Act for

DHS/CBP – 017 Analytical Framework for Intelligence (AFI) System of Records. Some information in AFI relates to official DHS national security, law enforcement, and immigration activities. The exemptions are required to preclude subjects from compromising an ongoing law enforcement, national security or fraud investigation; to avoid disclosure of investigative techniques; to protect the identities and physical safety of confidential informants and law enforcement personnel; and to ensure DHS's ability to obtain information from third parties and other sources.

Pursuant to 5 U.S.C. § 552a(j)(2), this system is exempted from the following provisions of the Privacy Act: 5 U.S.C. § 552a(c)(3) and (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5), (e)(8); (f); and (g). Additionally, pursuant to 5 U.S.C. § 552a(k)(1) and (2) this system is exempted from the following provisions of the Privacy Act: 5 U.S.C. § 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H); and (f). Many of the functions in this system require retrieving records from law enforcement systems. Where a record received from another system has been exempted in that source system under 5 U.S.C. § 552a(j)(2), (k)(1) and/or (k)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions in accordance with this rule.

The exemptions proposed here are standard for agencies where the information may contain investigatory materials compiled for law enforcement purposes. These exemptions are exercised by executive federal agencies. In appropriate circumstances, where compliance would not appear to interfere with or adversely affect the overall law enforcement process, the applicable exemptions may be waived on a case-by-case basis.

A notice of system of records for DHS/CBP – 017 Analytical Framework for Intelligence (AFI) is also published in this issue of the Federal Register.

II. Privacy Act:

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which the U.S. Government collects, maintains, uses, and disseminates personally identifiable information. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all persons, regardless of citizenship, where a system of records maintains information on both U.S. citizens and lawful permanent residents, as well as visitors.

The Privacy Act allows government agencies to exempt systems of records from certain provisions of the Act. If an agency claims an exemption, however, it must issue a Notice of Proposed Rulemaking and a Final Rule to make clear to the public the reasons why a particular exemption is claimed.

List of Subjects in 6 CFR Part 5

Freedom of information; Privacy.

For the reasons stated in the preamble, DHS proposes to amend Chapter I of Title 6, Code of Federal Regulations, as follows:

PART 5--DISCLOSURE OF RECORDS AND INFORMATION

1. The authority citation for Part 5 continues to read as follows:

Authority: Pub. L. 107–296, 116 Stat. 2135; (6 U.S.C. 101 et seq.); 5 U.S.C. § 301. Subpart A also issued under 5 U.S.C. 552. Subpart B also issued under 5 U.S.C. § 552a.

2. Add at the end of Appendix C to Part 5, the following new paragraph "68":

Appendix C to Part 5 – DHS Systems of Records Exempt From the Privacy Act

* * * * *

68. The DHS/ CBP—017 Analytical Framework for Intelligence (AFI) System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/CBP—017 Analytical Framework for Intelligence (AFI) System of Records is a repository of information held by DHS to enhance DHS's ability to: identify, apprehend, and/or prosecute individuals who pose a potential law enforcement or security risk; aid in the enforcement of the customs and immigration laws, and other laws enforced by DHS at the border; and enhance United States security. This system also supports certain other DHS programs whose functions include, but are not limited to, the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. The DHS/CBP—017 Analytical Framework for Intelligence (AFI) System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from certain provisions of the Privacy Act as follows:

- Pursuant to 5 U.S.C. § 552a (j)(2), the system is exempt from 5 U.S.C. § 552a (c)(3) and (c)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g).
- Pursuant to 5 U.S.C. § 552a (j)(2), the system (except for any records that were ingested by AFI where the source system of records already provides access and/or amendment under the Privacy Act) is exempt from 5 U.S.C. § 552a (d)(1), (d)(2), (d)(3), and (d)(4).
- Pursuant to 5 U.S.C. § 552a (k)(1), the system is exempt from 5 U.S.C. § 552a(c)(3); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f).
- Pursuant to 5 U.S.C. § 552a (k)(1), the system is exempt from (d)(1), (d)(2), (d)(3), and (d)(4).
- Pursuant to 5 U.S.C. § 552a (k)(2), the system is exempt from 5 U.S.C. § 552a(c)(3); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f).
- Pursuant to 5 U.S.C. § 552a (k)(2), the system (except for any records that were ingested by AFI where the source system of records already provides access and/or amendment under the Privacy Act) is exempt from (d)(1), (d)(2), (d)(3), and (d)(4).

Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the

recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement and national security, it is

appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement and national security activities.

(e) From subsection (e)(3) (Notice to Individuals) because providing such detailed information could impede law enforcement and national security by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete.

Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

Dated: June 4, 2012

Mary Ellen Callahan

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2012-13815 Filed 06/06/2012 at 8:45 am; Publication Date: 06/07/2012]