This document is scheduled to be published in the
Federal Register on 09/18/2013 and available online at
http://federalregister.gov/a/2013-22690, and on **FDsys.gov**

9111-14 (non-Treasury)

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2013-0021]

Privacy Act of 1974; Department of Homeland Security/U.S. Customs and Border Protection - 019 Air and Marine Operations Surveillance System (AMOSS) System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to establish a new Department of Homeland Security system of records titled, "Department of Homeland Security/U.S. Customs and Border Protection - 019 Air and Marine Operations Surveillance System (AMOSS) System of Records." This system of records allows the Department of Homeland Security/U.S. Customs and Border Protection to collect and maintain records on publicly available aircraft and airport data provided by the Federal Aviation Administration (FAA), requests from law enforcement about suspects, tips from the public, and recordings of event and operations data in a watch log or event tracking log. Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act, elsewhere in the Federal Register. This newly established system will be included in the Department of Homeland Security's inventory of record systems.

DATES AND COMMENTS: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This new system will be effective [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2013-0021 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Jonathan R. Cantor, Acting 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 rulemaking. 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 Castelli, (202) 325-0280, Privacy Officer, U.S. Customs and Border Protection, Washington, DC 20229. For privacy issues please contact: Jonathan R. Cantor, (202) 343-1717, Acting 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/CBP - 019 Air and Marine Operations Surveillance System (AMOSS) System of Records."

This System of Records Notice (SORN) is being published because AMOSS stores personally identifiable information in a system of records. AMOSS is a sophisticated radar processing system that supports the concerted and cooperative effort of air, land, and sea vehicles; field offices; and command and control centers staffed by law enforcement officers (LEO), detection enforcement officers (DEO), pilots, crew, and Air and Marine Operations Center (AMOC) support staff in monitoring approaches to the U.S. border to detect illicit trafficking and direct interdiction actions, as appropriate. AMOSS also supports domestic operations in conjunction with other domestic law enforcement agencies by tracking domestic flights, as well as providing air traffic monitoring for air defense purposes. By processing a collection of external data imposed over a zooming-capable screen, AMOSS provides a real-time picture of air activity over a wide portion of North America, thus allowing system operators to discriminate between normal and suspicious air, ground, and marine vehicle movement. Much of the external data processed by AMOSS does not contain Personally Identifiable Information (PII) and is supplied to AMOSS by means of networked external sources. For instance, global positioning systems (GPS) from CBP vehicles or law enforcement investigations, maps, datasets from radar plot data, track data, and flight plan data are all incorporated to enhance the system operator's ability to differentiate between normal and suspicious aviation movement.

AMOSS collects PII principally from the following sources:

(1) Aircraft registration and owner information, which is downloaded to AMOSS weekly from the publicly available Federal Aviation Administration (FAA) Registration Database (DOT/FAA-801 - Aircraft Registration System (April 11, 2000, 65 FR 19518));

(2) Airport manager contact information, which is contained in a larger download of airport and aeronautical navigation data obtained from the FAA National Flight Data Center website (DOT/FAA- 847 - Aviation Records on Individuals (November 9, 2010, 75 FR 68849));

(3) Suspect information entered into the AMOC watch or event track logs received from other CBP personnel or law enforcement agencies; and

(4) Information from members of the public who call in to report suspicious activity to a tip line.

The majority of the PII contained in AMOSS is publicly available data, which AMOSS downloads from the FAA Registration Database. The FAA Registration Database contains airport and runway information, aircraft registration (ownership) information on U.S. registered aircraft, flight plan/route information, special use airspace identification, and navigation aids identification. The information that AMOSS extracts from the FAA Registration Database contains PII in the form of aircraft owner names and addresses and airport manager names and phone numbers.

AMOSS also contains event and operations data, which DEOs or other AMOC staff record in a watch log or event tracking log. The watch log contains records of operational activities on the floor of the AMOC. The event tracking log contains active

event logs of all investigative and law enforcement actions in response to suspicious activity. The watch log and event tracking log are similar to a police blotter or journal and can include intelligence/suspect records on vehicles, vessels, and aircraft, as well as airport manager names and phone numbers. In addition, the watch log and event tracking log may contain PII of suspects who are encountered when the DEOs are investigating suspicious air, ground, and marine vehicle movement, including names, addresses, phone numbers, drivers licenses, and, in some cases, Social Security Numbers (SSN) of suspects. The watch log and event tracking log may also contain PII from members of the public who call in to a tip line to report tips on suspicious activity, including names and phone numbers. Consistent with DHS's information sharing mission, information stored in AMOSS may be shared with other DHS components when CBP has determined that the component has a need to know the information. In addition to CBP, AMOSS has users from various DHS components including the U.S. Immigration and Customs Enforcement (ICE), U.S. Secret Service (USSS), and the Transportation Security Administration (TSA). Based on a need to know, CBP may share data from AMOSS with other parts of DHS including, but not limited to, the DHS National Operations Center, U.S. Coast Guard (USCG), and the Office of Intelligence and Analysis (I&A). Information is transmitted via secure connections between components.

When appropriate, information in AMOSS may be included in a Memorandum of Information Received (MOIR) in TECS (DHS/CBP-011 - U.S. Customs and Border Protection TECS (December 19, 2008 73 FR 77778)) and shared as a suspicious activity report, pursuant to DHS/ALL-031 - Information Sharing Environment Suspicious Activity Reporting Initiative (September 10, 2010, 75 FR 55335).

DHS may share with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies when DHS determines that the receiving component has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice. AMOSS also has users from the Department of Defense (DOD), including the North American Aerospace Defense Command (NORAD). NORAD users include members of the Canadian Armed Forces. These users use AMOSS to identify and track aircraft that are transiting, entering, and departing from the United States. Access for these users is restricted through the use of role-based assignments within AMOSS.

As part of the AMOC's law enforcement and general aviation security mission, non-PII aircraft positional data may be shared with other foreign, federal, state, and local agencies. Upon request, AMOSS also supports domestic operations in conjunction with other domestic law enforcement agencies by tracking domestic flights.

The collection of information in AMOSS is authorized primarily by the following authorities: 6 U.S.C. § 202; the Tariff Act of 1930, as amended, including 19 U.S.C. § 1590; 19 U.S.C. § 2075(b)(2)(B)(3); the Immigration and Nationality Act (INA), 8 U.S.C. § 1101, *et seq.*, including 8 U.S.C. §§ 1103, 1225, and 1324; and the Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. 104-208; Presidential Directive 47/Homeland Security Presidential Directive 16 (NSPD-47/HSPD-16); and DHS Delegation No. 7010.3 (May 11, 2006).

DHS is issuing a Notice of Proposed Rulemaking, elsewhere in the Federal Register, to exempt this system of records from certain provisions of the Privacy Act.

CBP will, however, consider individual requests to determine whether or not information may be released. Moreover, no exemption shall be asserted with respect to information maintained in the system as it relates to aircraft data collected from the FAA, aside from the accounting of disclosures with law enforcement and/or intelligence agencies pursuant to the routine uses in this SORN. This newly established system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which federal government agencies collects, maintains, uses, and disseminates individuals' records. 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 an 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 individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

Below is the description of the DHS/CBP-019 Air and Marine Operations Surveillance System (AMOSS) System of Records.

In accordance with 5 U.S.C. § 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

System of Records

DHS/CBP - 019

System name:

DHS/U.S. Customs and Border Protection - 019 Air and Marine Operations Surveillance System (AMOSS).

Security classification:

Unclassified, sensitive, and law enforcement sensitive.

System location:

Records are maintained at the Air and Marine Operations Center (AMOC) in Riverside, California.

Categories of individuals covered by the system:

AMOSS contains information on aircraft owners who have registered their aircraft with the Federal Aviation Administration (FAA), as well as airport managers. AMOSS contains information about individuals suspected of violating the law or presenting a threat to the United States. AMOSS also contains information about individuals mentioned in tips from members of the public who call in to report suspicious activity to a tip line or from law enforcement, as well as contact information for those members of the public or law enforcement.

Categories of records in the system:

The records in AMOSS are comprised of the following information:

FAA DATA:

- Aircraft registration (ownership) information on U.S. registered aircraft, including registrant name and address, aircraft type, and aircraft identification numbers;
- Airport information, including manager name and contact information;

- Runway information;
- Flight plan/route information;
- Special use airspace identification; and
- Navigation aids identification.

EVENT AND OPERATIONS DATA:

- Watch log records of operational activities on the floor of the AMOC;
- Event tracking log information on suspects, including: names, addresses, phone numbers, drivers licenses, Social Security Numbers, TECS case numbers, information identifying conveyances (including vehicle type, tail numbers, license plate numbers, etc.) and remarks by Detection Enforcement Officers (DEO);
- Event tracking log information on members of the public who call in to a tip line, including: names, and phone numbers.

Authority for maintenance of the system:

The collection of information in AMOSS is authorized by the following authorities: 6 U.S.C. § 202; the Tariff Act of 1930, as amended, including 19 U.S.C. § 1590; 19 U.S.C. § 2075(b)(2)(B)(3); the Immigration and Nationality Act ("INA"), 8 U.S.C. § 1101, *et seq.*, including 8 U.S.C. §§ 1103, 1225, and 1324; the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. 104-208, Division C; Presidential Directive 47/Homeland Security Presidential Directive 16 (NSPD-47/HSPD-16); and DHS Delegation No. 7010.3 (May 11, 2006).

Purpose(s):

Information in AMOSS is used to assist CBP in identifying aircraft, vessels, or vehicles illegally entering or attempting to enter the United States, making suspicious movements, or otherwise participating in the smuggling or transshipment of narcotics, illegal contraband, illegal aliens, illegal currency, terrorist activities, or other suspected or confirmed violations of U.S. customs and/or immigration laws. Information in AMOSS is also used to assist other foreign, federal, state, and local agencies for law enforcement and general aviation security purposes.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. § 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including U.S. Attorney Offices, or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an

inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. DHS has determined that as a result of the suspected or confirmed compromise, there is a risk of identity theft or fraud, harm to economic or property interests, harm to an individual, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to

the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To federal and foreign government intelligence or counterterrorism agencies or components when DHS becomes aware of an indication of a threat or potential threat to national or international security, or to assist in anti-terrorism efforts.

I. To an organization or person in either the public or private sector, either foreign or domestic, when there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, or when the information is relevant to the protection of life, property, or other vital interests of a person.

J. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation.

K. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil or criminal discovery, litigation, or settlement negotiations, or in response to a subpoena from a court of competent jurisdiction.

L. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations when CBP is aware of a need to use relevant data for purposes of testing new technology and systems designed to enhance border security or identify other violations of law.

M. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on magnetic disc, tape, digital media and DVD/CD-ROM.

Retrievability:

Records may be retrieved by name or other (alphanumeric) personal identifier.

Safeguards:

Records in this system are safeguarded in accordance with applicable rules and

policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

Retention and disposal:

CBP has established a 15-year retention schedule beginning on the last date of the record entry or update, and plans to submit this schedule to NARA for approval.

System Manager and address:

Director, Information Systems, U.S. Customs and Border Protection, Office of Air and Marine, Air and Marine Operations Center, Riverside, California.

Notification procedure:

The Secretary of Homeland Security has exempted portions of AMOSS from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. CBP will, however, consider individual requests to determine whether or not information may be released. Moreover, no exemption shall be asserted with respect to information maintained in the system as it relates to aircraft data collected from the FAA, aside from the accounting of disclosures with law enforcement and/or intelligence agencies pursuant to the routine uses in this SORN. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the CBP FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "contacts." If an individual believes more than one component maintains Privacy Act records concerning

him or her the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0655, Washington, D.C. 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov or 1-866-431-0486. In addition you should:

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

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

Record access procedures:

See "Notification procedure" above.

Contesting record procedures:

See "Notification procedure" above.

Record source categories:

Records containing PII are obtained from the following sources:

(1) Aircraft registration and owner information from the publicly available FAA Registration Database;

(2) Airport manager contact information, which is contained in a larger download of airport and aeronautical navigation data obtained from the FAA National Flight Data Center;

(3) Suspect information entered into the AMOC watch or event track logs received from other CBP personnel or law enforcement agencies; and

(4) Information from members of the public who call in to report suspicious activity to a tip line.

Exemptions claimed for the system:

No exemption shall be asserted with respect to aircraft data collected from the FAA that is maintained in AMOSS. However, this FAA data may be shared with law enforcement and/or intelligence agencies pursuant to the above routine uses. The Privacy Act requires DHS maintain an accounting of the disclosures made pursuant to all routine

uses. Disclosing the fact that a law enforcement or intelligence agency has sought particular records may affect ongoing law enforcement or intelligence activity. As such, pursuant to 5 U.S.C. § 552a(j)(2), DHS will claim an exemption from subsections (c)(3); (e)(8); and (g)(1) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information. Further, DHS will claim exemption from subsection (c)(3) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. § 552a(k)(2) as is necessary and appropriate to protect this information.

The Secretary of Homeland Security, pursuant to 5 U.S.C. § 552a(j)(2), has exempted all other AMOSS data (non-FAA source data) from the following provisions of the Privacy Act: 5 U.S.C. § 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), and (e)(8); (f); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. § 552a(k)(2), has exempted this non-FAA source data in AMOSS from the following provisions of the Privacy Act: 5 U.S.C. § 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). When a record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(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 set forth here.

Dated: August 6, 2013

Jonathan R. Cantor

Acting Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2013-22690 Filed 09/17/2013 at 8:45 am; Publication Date: 09/18/2013]