



Privacy Impact Assessment
for the

**Air and Marine Operations
Surveillance System (AMOSS)**

DHS/CBP/PIA-019

August 8, 2013

Contact Point

Tony Crowder

Executive Director, Air and Marine Operations Center (AMOC)

Office of Air and Marine

U.S. Customs and Border Protection

(951) 656-8001

Reviewing Official

Jonathan R. Cantor

Acting Chief Privacy Officer

Department of Homeland Security

(202) 343-1717



Abstract

The Air and Marine Operations Surveillance System (AMOSS) is a sophisticated radar processing system that supports the Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP) mission to protect the American people and critical infrastructure. AMOSS integrates use of air, land, and sea resources in order to detect, interdict, and prevent acts of terrorism and the unlawful movement of people, illegal drugs, and other contraband toward or across the borders of the United States. AMOSS is operated by the Air and Marine Operations Center (AMOC), a component of the CBP Office of Air and Marine (OAM), and may collect and use personally identifiable information (PII) from 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. This Privacy Impact Assessment (PIA) is being conducted to provide notice and transparency to the public that AMOSS collects, uses, and shares PII.

Overview

The Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP) is issuing this Privacy Impact Assessment (PIA) for the Air and Marine Operations Surveillance System (AMOSS). AMOSS is operated by the Air and Marine Operations Center (AMOC), a component of the CBP Office of Air and Marine (OAM). AMOC was established in 1988 as a state-of-the-art law enforcement radar surveillance center designed to counter the on-going threat of airborne drug smuggling. AMOC has expanded its role in air and marine interdiction and, following the September 11, 2001, terrorist attacks, has used its extensive detection, monitoring, and coordination capabilities to conduct airspace security operations, covert and overt electronic tracking, and general aviation aircraft threat determination. Through the use of AMOSS, AMOC is able to fulfill its law enforcement mission. This PIA pertains to CBP's collection and use of personally identifiable information (PII) through AMOSS.

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 AMOC support staff in monitoring approaches to the U.S. border to detect illicit trafficking and direct interdiction actions, as appropriate. 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 CBP system operators to differentiate between normal and suspicious air, ground, and marine vehicle movement.

Much of the external data processed by AMOSS does not contain 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 maintains PII 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;¹
- (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 every 56 days;²
- (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 1-866-AIR BUST (1-866-247-2878) to report suspicious activity.

FAA Data

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.

Event and Operations Data

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 at 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 1-866-AIR BUST to report tips on suspicious activity, including names and phone numbers. If suspicious activity is reported through AMOSS that is reasonably indicative of terrorist activity, this information may be included in a Memorandum of Information Received (MOIR) in TECS and incorporated as a suspicious activity report, pursuant to DHS/ALL-031 - Information Sharing Environment Suspicious Activity Reporting Initiative System of Records Notice (SORN) (September 10, 2010, 75 FR 55335). TECS serves as a data repository to support law enforcement, border screening, and reporting for CBP's primary and secondary inspection processes.

A typical AMOC transaction using AMOSS to track a suspicious flight would be as follows: A DEO receives flight plan movement information, populated from publicly available FAA records, on an

¹ SORN: DOT/FAA-801 - Aircraft Registration System (April 11, 2000, 65 FR 19518); PIA available at: <http://www.dot.gov/individuals/privacy/pia-airmenaircraft-registry-modernization-system>.

² SORN: DOT/FAA-847 - Aviation Records on Individuals (November 9, 2010, 75 FR 68849); PIA available at: <http://www.dot.gov/individuals/privacy/pia-airmenaircraft-registry-modernization-system>.



aircraft that has been previously suspected of possible narcotics trafficking. The DEO will review the flight route information and related case information in other law enforcement systems and verify whether the case agent for this specific aircraft needs notification of the movement, as appropriate. The DEO will take the appropriate actions and log these actions in the watch log or the event tracking log. Because radar has some limited ground detection capabilities, similar procedures are followed when a ground vehicle is detected and referred to the Office of Border Patrol. An official case file may or may not exist at this point in time.

Another way an AMOSS transaction would occur is during a “cold detection,” when a DEO is observing a radar track (e.g., aircraft or maritime vessel) that crosses the border or the territorial waters of the United States.

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.

AMOSS provides limited user accounts to the Department of Defense (DOD), including the North American Aerospace Defense Command (NORAD) and 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, and have access to the radar tracking and publicly available data within the FAA airport and registration tables. These users are not granted access to AMOSS sensitive law enforcement database tables, such as the watch log, event tracking log, and suspect/intelligence records.

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. Such sharing is recorded in the AMOSS watch log and only contains the publicly available take-off, flight path, radar, and landing information for a requested plane number. Separate from AMOSS, the AMOC also supports domestic law enforcement operations in conjunction with other domestic law enforcement agencies by providing TECS records for individuals associated with a plane number, upon request. These external requests must contain an official need to know and comply with the routine uses in the TECS SORN,³ and any sharing of TECS records is documented through a DHS-191 Privacy Act Disclosure Record in addition to being noted in the AMOSS watch log. If the TECS records were created by ICE, the AMOC will refer the request for records to the originating office within ICE.

³ DHS/CBP-011 - U.S. Customs and Border Protection TECS (December 19, 2008, 73 FR 77778).



Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

AMOSS derives its authority primarily from 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).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

FAA data comes from the DOT/FAA-801 - Aircraft Registration System (April 11, 2000, 65 FR 19518) and the DOT/FAA-847 - Aviation Records on Individuals (November 9, 2010, 75 FR 68849) SORNs. CBP is publishing the Air and Marine Operations Surveillance System of Records Notice, DHS/CBP-019, concurrent with this PIA. When appropriate, information in AMOSS may be used in an MOIR and included in a suspicious activity report, pursuant to DHS/ALL-031 - Information Sharing Environment Suspicious Activity Reporting Initiative (September 10, 2010, 75 FR 55335).

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. The Authority to Operate (ATO) is complete as of December 05, 2012, and expires in December 2015.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

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

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

FAA Registration Database information maintained by AMOSS is initially collected by the FAA, with the OMB control number and agency number for collection on their official forms: OMB 2120 0024, 0042, 0690, 0697, and 0729. There is no standard information collection from members of the public or from requesting agencies that call in to report a suspicious aircraft. Rather, information received from members of the public or requesting agencies is entered in narrative form into the text fields of the event tracking log.



Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The majority of PII in AMOSS is publicly available data which AMOSS downloads from the FAA Registration Database. Other data contained in AMOSS is event and operations data. Within these types of data collected, AMOSS contains the following PII:

- (1) Aircraft registration and owner information, downloaded to AMOSS weekly from the publicly available FAA Registration Database;
- (2) Airport manager contact information, contained in a larger download of airport and aeronautical navigation data obtained from the FAA National Flight Data Center's public website every 56 days;
- (3) Suspect information entered into the AMOC watch or event track logs that is 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 1-866-AIR-BUST.

FAA Data

AMOSS downloads publicly available aircraft data from the FAA Registration Database, including 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. FAA data contains PII in the form of aircraft owner names and addresses and airport manager names and phone numbers.

Event and Operations Data

AMOSS also collects 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 at 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, SSNs of suspects. Some of this information may be cross-referenced in TECS and entered into AMOSS. The watch log and event tracking log may also contain PII from members of the public who call in to 1-866-AIR-BUST to report suspicious activity, including names and phone numbers.



2.2 What are the sources of the information and how is the information collected for the project?

The information within AMOSS comes from the following sources: the FAA, law enforcement, and private citizen reports. The FAA's publicly available data is downloaded from the FAA's website and includes information on aircraft registration, airport managers/owners, and other national airspace infrastructure information. Various federal and state law enforcement officers provide law enforcement case information on active suspects or vehicles to DEOs or other AMOC staff, who manually enter the information into the event tracking log. External parties (federal, state, and local law enforcement officers), CBP Officers and Agents in the field, or DEOs at the AMOC can identify an individual or a flight pattern as suspicious, thereby prompting the DEO to start an event tracking log. The event tracking logs have phone numbers for law enforcement officers who have notified the DEOs of the case information.

Private citizen reports of suspected illegal or suspicious activity are entered manually into the watch log by the DEOs or other AMOC staff. These tips include the detailed narrative statement from the citizen regarding the suspicious activity and, if the citizen provides his or her call back information, the citizen's name and phone number. Such citizen reports are made through calls to a toll-free line, 1-866-AIR-BUST, which OAM places on public signage near border areas.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Yes. FAA aircraft registration and airport tables are populated from data that is available to the general public on the FAA website to aid in efficient air travel.

2.4 Discuss how accuracy of the data is ensured.

AMOSS receives aircraft registration data from the FAA Registration Database, which collects the information directly from persons registering an aircraft. Tip information received from the public is evaluated by DEOs as part of the process for identifying suspicious or illegal activity. Case information from law enforcement agencies is evaluated for accuracy as part of AMOC operations process. In addition, information contained in AMOSS is regularly reviewed by the DEO and Supervisory DEO to ensure the information is accurate and complete at all times throughout the operation.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that some PII collected is not directly relevant and necessary for AMOSS to accomplish its mission.

Mitigation: AMOSS supports the concerted and cooperative effort to monitor approaches to the U.S. border to detect illicit trafficking and direct interdiction actions, as appropriate. All information downloaded from the FAA, received from CBP or law enforcement agencies, or submitted by the public to report a suspicious activity has a nexus to CBP's law enforcement mission at the border or generally



supports aviation or marine security. In addition, the effectiveness of authentication and security protections are verified through audits of system operation and usage.

Privacy Risk: There is a privacy risk that some PII collected will not be accurate and timely.

Mitigation: Information downloaded from the FAA Registration database is originally submitted by the person registering an aircraft. The accuracy of the information depends on the person submitting the registration to the FAA. Should a person contact the FAA to change or update his or her registration information, that change will be reflected in the weekly FAA feed downloaded by AMOSS. There is a risk that information will remain inaccurate in AMOSS during that weekly period, but technical limitations prevent a real-time update.

Event-driven PII in AMOSS is timely because it is a snapshot of data that is collected at the time of the event, such as a law enforcement stop or arrest. In documenting an event, the DEO may enter suspect data into the watch log or event tracking log. This data may include information from the suspect's identification card; intelligence; or air, ground, or marine vehicle alerts derived from a wants/warrants lookout. Voluntarily provided PII includes contact information (e.g., name and phone number) that a law enforcement officer or private citizen may provide to law enforcement authorities when reporting suspicious activity and is presumed to be correct since it is collected directly from the individual. Information provided by the law enforcement officer or private citizen is evaluated for accuracy as part of AMOC operations.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

AMOSS compares the data it receives from the FAA with a real-time picture of air activity over a wide portion of North America by processing a collection of external data imposed over a zooming-capable screen. This picture, combined with the tips from the public and investigative notes from DEOs, allows system operators to discriminate between normal and suspicious air, ground, and marine vehicle movement. The ability to detect suspicious movement assists the AMOC in identifying aircraft, vessels, or vehicles illegally entering the United States or involved in the transshipment or carrying of narcotics, illegal contraband, illegal aliens, illegal currency, terrorist activities, or other suspected or confirmed violations of customs or immigration law.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. AMOSS uses searches and queries for routine data retrieval of information from the FAA database tables and to determine whether a flight has deviated from its reported flight plan.



3.3 Are there other components with assigned roles and responsibilities within the system?

Yes. In addition to CBP, AMOSS has users from various DHS components including ICE, USSS, and 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, USCG, and DHS I&A. Information is transmitted via HSIN or HSDN.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that some PII collected may be used for a purpose unrelated to the mission AMOSS.

Mitigation: Use of information in AMOSS is strictly limited to that which is relevant to the law enforcement and aviation security missions of the system. Data is used to identify and/or confirm potential violations of customs or immigration law, investigate potential terrorist threats or otherwise support general aviation security, and support law enforcement agencies by tracking domestic flights. Specifically, data is used in identifying aircraft, vessels, or vehicles illegally entering the United States or involved in the illegal transshipment or carrying of narcotics, contraband, aliens, currency, terrorist activities, or other suspected or confirmed violations of customs or immigration law. 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 law enforcement operations in conjunction with other domestic law enforcement agencies by tracking domestic flights. All sharing of information is documented through the AMOSS watch log. All user access (including non-CBP user access) to AMOSS is limited according to the user's assigned role.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

DHS/CBP provides general notice of its law enforcement activities through this PIA and the publishing of a new system of records notice, DHS/CBP – 019 AMOSS. Individuals providing tip information through 1-866-AIR BUST are notified that their information is treated as law enforcement information and kept confidential. For information downloaded from the FAA Registration Database, notice of the FAA's collection is provided in the form of a Privacy Act Statement at the original point of collection, and described in the PIA and SORN associated with the FAA database.⁴ Both FAA SORNs

⁴ For a detailed description of the notice provided at the point of collection for the FAA, please see the Airmen/Aircraft Registry Modernization System (RMS) PIA, available at <http://www.dot.gov/individuals/privacy/pia-airmenaircraft-registry-modernization-system>, and the corresponding Department of Transportation System of Records Notices, DOT/FAA 847 -



provide routine uses permitting the sharing of the data for investigation and law enforcement purposes.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Any individual who owns an aircraft is required by federal law to register the aircraft in accordance with FAA regulations. This information is publicly available. Individuals do not have a right to consent or decline to this use of information. Any individual who chooses to operate an aircraft over United States airspace does so in accordance with federal law and implementing regulations and consents to being tracked by radar to ensure aviation safety and security. Furthermore, individuals who are interdicted in the course of an aviation or maritime border security enforcement action also do not have an opportunity to consent or decline to provide their information.

Individuals who contact 1-866-AIR-BUST do have an opportunity to consent or decline to the collection of information. Calling AMOC to report suspicious aviation activity is not required, and all information submitted to AMOC is voluntary. Individuals may choose to remain anonymous.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not be aware that CBP is collecting information on their activity.

Mitigation: CBP does not provide notice to the individual because of the law enforcement nature of the system. Providing notice to individuals about the operations in AMOSS would frustrate CBP's ability to investigate possible violations and detect threats at the border. CBP is publishing this PIA and DHS/CBP-019 AMOSS SORN to increase the transparency of its operations. In addition, notice is provided to individuals by the FAA through the publication of DOT/FAA 847 Aviation Records on Individuals SORN and DOT/FAA 801 Aircraft Registration System SORN, which contain routine uses for law enforcement sharing.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

Aircraft registration and owner information obtained from the publicly available FAA Registration Database is overwritten and updated weekly. Airport manager contact information from the FAA National Flight Data Center is overwritten and updated every 56 days. Information from these databases incorporated into an AMOSS record and all other data is maintained for 15 years from the last date of the record entry or update to assist with future law enforcement and border security operations. When information is shared with another system, it will be retained in accordance with the retention period for records in that system.



5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that AMOSS retains PII longer than necessary.

Mitigation: This risk is mitigated by the requirement that all data be deleted no later than 15 years from the last date of the record entry or update. Fifteen years was determined to be an appropriate length of time for all AMOC personnel to complete their law enforcement duties and rely on historical information, without retaining information unnecessarily or indefinitely. AMOSS allows for automated purging of PII; however, manual purging will be used to maintain maximum control over the purge process and ensure that sensitive data is not accidentally purged.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government and private sector entities.

6.1 **Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.**

DHS/CBP shares AMOSS information primarily at the federal law enforcement level. Law enforcement data sharing may occur on a specific case-by-case basis with state, local, tribal, foreign, or international government agencies and task forces that have a need to know the information.

Sharing Non-PII Aircraft Positional Data:

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. Such sharing is recorded in the AMOSS watch log and only contains the publicly available take-off, flight path, radar, and landing information for a requested plane number.

Sharing Other AMOSS Data:

AMOSS information is also shared on an as-needed basis with intelligence agencies or fusion centers that are lawfully engaged in collecting and producing law enforcement intelligence. AMOSS information is shared with other federal agencies in the course of collaborating, assisting, and supporting national intelligence and security investigations by incorporating AMOSS data into a MOIR in TECS.⁵

In the event that a suspicious air, ground, or marine vehicle movement is detected and the DEO determines that interdiction is required, the information collected in AMOSS may be shared throughout CBP and DHS, as well as with other federal agencies, including FAA for flight tracking purposes, DOD and Canadian Armed Forces for military defense and security purposes, Federal Bureau of Investigation (FBI) for law enforcement purposes, Drug Enforcement Administration (DEA) for drug smuggling interdiction, and various other law enforcement organizations on a case-by-case basis consistent with a

⁵ See DHS/ALL/PIA-032 Department of Homeland Security Information Sharing Environment Suspicious Activity Reporting Initiative (November 17, 2010).



law enforcement purpose. Information may also be shared with the Department of State (DOS) for use by Consular Officers at U.S. Embassies and Consulates. Information containing PII that is transmitted electronically to external organizations is accomplished separately via CBP/DHS approved secured Law Enforcement Information Sharing Service connections. Sensitive law enforcement information is not shared via access to AMOSS databases.

Sharing Associated TECS Records:

Separate from AMOSS, the AMOC also supports domestic law enforcement operations in conjunction with other domestic law enforcement agencies by providing TECS records for individuals associated with a plane number, upon request. These requests must contain an official need to know and comply with the routine uses in the TECS SORN.⁶ Any sharing of TECS records is documented through a DHS-191 Privacy Act Disclosure Record in addition to being noted in the AMOSS watch log. If the TECS records were created by ICE, the AMOC will refer the request for records to the originating office within ICE.

Non-DHS Access to AMOSS:

All non-DHS agencies have signed an Information Sharing Access Agreement (ISAA) or Memorandum of Understanding (MOU) prior to being granted access to AMOSS and all users have signed Rules of Behavior. AMOSS has non-DHS users from the DOD, including the North American Aerospace Defense Command (NORAD). Among the NORAD users are members of the Canadian armed forces. Users from these agencies 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. These users have access to the publicly available data within the FAA airport and registration tables; however, they are not granted access to AMOSS's sensitive law enforcement database tables, such as the watch log, event tracking log, and suspect/intelligence records that contain sensitive PII. DOD secures AMOSS information in accordance with the terms of CBP/DHS approved information sharing agreements, which include provisions for appropriate and adequate safeguarding of sensitive information.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The sharing described above is compatible with the original purpose for collection, namely to support the concerted and cooperative effort to monitor air, land, and sea approaches to the U.S. border and all air traffic over the United States to detect violations of U.S. law or possible threats to the United States, to direct appropriate law enforcement interdiction actions, and to support general aviation security.

6.3 Does the project place limitations on re-dissemination?

Under the terms of the sharing arrangement, whether by MOU/ISAA or case-by-case basis, PII shared from AMOSS is law enforcement sensitive data and is prohibited from being re-disseminated without CBP's express authorization.

⁶ DHS/CBP-011 - U.S. Customs and Border Protection TECS (December 19, 2008, 73 FR 77778).



6.4 Describe how the project maintains a record of any disclosures outside of the Department.

All disclosures of PII from AMOSS are documented. All information releases are logged in either the watch logs or event tracking logs. All external sharing of PII is documented on the Privacy Act Disclosure Record (DHS Form 191), which notes the name of the individual whose records are requested, the system from which the records are taken, the nature of the disclosure, and the name of the requestor.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that AMOSS information may be shared with those who do not have a need to know the information or in a manner that is inconsistent with the routine uses in DHS/CBP-019 AMOSS SORN.

Mitigation: Information is transmitted via DHS e-mail or over secure connections or hand-delivery to DHS special agents, supporting analysts, supervisors, and other authorized DHS law enforcement, intelligence, and counterterrorism agencies, on a need-to-know basis. All external users of AMOSS with access to PII are required to be trained on the requirements of the Privacy Act and in appropriate use and disclosure controls pertinent to the information. PII transmitted or disclosed within DHS is password protected. DOD/NORAD (including Canadian Armed Forces) users only have access to the publicly available data within the FAA airport and registration tables; they are not granted access to AMOSS's sensitive law enforcement database tables, such as the watch log, event tracking log, and suspect/intelligence records that contain sensitive PII. There is a limited risk of exposure of information contained in the release records by internal partners since the partners are law enforcement entities with equal or greater restrictions on the release of PII. Information shared with these partner entities is consistent with the original purpose of collection, or for a law enforcement purpose, and is consistent with the routine uses in the DHS/CBP-019 AMOSS SORN.

Privacy Risk: There is a privacy risk that PII in the system may be accessed or altered by unauthorized individuals for criminal or other unauthorized purposes.

Mitigation: This privacy risk is minimized by the AMOSS architecture, which maintains the limited amount of PII data in a single data repository and system rather than in separate applications and systems in different locations. This structure reduces the privacy risk to the data by minimizing its proliferation in multiple locations and systems, each of which would need to employ physical or technological security measures to prevent a breach. Authentication and role-based user access requirements ensure that users can only access or change AMOSS information that is appropriate for their official duties. AMOC supervisors determine the user roles and access requirements of their subordinates, and a user account may only be established after written supervisory approval is provided. In addition, background checks are conducted on users to ensure they are suitable for authorized access to AMOSS. The effectiveness of authentication and security protections are verified through audits of system operation and usage.



Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

The Secretary of Homeland Security has exempted portions of AMOSS from the notification and access 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 the AMOSS SORN.

Under the Privacy Act and the Freedom of Information Act (FOIA) individuals may request administrative access to the information they provide that is maintained in the applicable CBP systems of records. Individuals seeking notification of and access to records contained in AMOSS or seeking to contest its content, may submit a FOIA or Privacy Act request with CBP at <https://foia.cbp.gov/palMain.aspx>, or by mailing a request to:

CBP FOIA Headquarters Office
U.S. Customs and Border Protection
FOIA Division
90 K Street NE, 9th Floor
Washington, DC 20002
Fax Number: (202) 325-0230

Requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. Specific FOIA contact information can be found at <http://www.dhs.gov/foia> under contacts.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The Secretary of Homeland Security has exempted portions of AMOSS, including the watch and event tracking logs, from the 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 amended. No exemption shall be asserted with respect to information maintained in the system as it relates to aircraft data collected from the FAA by submitting a Privacy Act Amendment Request to the CBP FOIA Headquarters Office, above. Such requests must conform to the requirements in 6 CFR Part 5. Individuals may also amend the data collected from the FAA through the procedures described in the FAA SORNs. Such amendments will then be incorporated into the AMOSS download of that data.

Because of the law enforcement nature of this system, private citizens are not system users and



are not able to directly access their information in AMOSS to correct it. Designated systems users do have the ability to annotate watch log and event tracking log record entries that are found to be in error after these records have been locked. Errors are typically determined either by the user's self-review, supervisory review, or by receiving further information on a case after the action report has been entered into the system.

7.3 How does the project notify individuals about the procedures for correcting their information?

This PIA and DHS/CBP-019 AMOSS SORN notifies individuals that requests to correct their information may be submitted in writing to the CBP FOIA Officer. See Section 7.1, above.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will not be aware of procedures in place for correcting AMOSS information on themselves.

Mitigation: Because of the law enforcement nature of this system, CBP does not have procedures to allow public access and amendment of certain records, including the watch logs or event tracking logs, in AMOSS. Providing such access and amendment would frustrate legitimate law enforcement investigations and detection of threats at the border. However, CBP may provide access and/or amendment to AMOSS records on a case-by-case basis through the procedures listed in Section 7.1 and 7.2, above. CBP will not assert an exemption 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 the AMOSS SORN.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

All actions are logged and audited in accordance with CBP and DHS policy. Access to AMOSS is restricted to secure locations with controlled access.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

General privacy training is accomplished through the annual DHS/CBP training for privacy, which is directly applicable to appropriate use of AMOSS.



8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Access requests are initiated and signed by the individual user's respective supervisor. AMOSS can only be accessed by authorized users with a user name and password that is uniquely assigned to the user. User access is documented through the use of a request process that also requires notice and termination of the account under conditions of separation or change of duties. Administrators have access to elevated privileges for the performance of their system administration and maintenance duties. Foreign users of AMOSS (members of the Canadian Armed Forces through NORAD) must go through an additional approval process through CBP and DHS before being given a role in the system.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

AMOC reviews and approves, if appropriate, requests for AMOSS access based upon requirements for a shared common operating picture (e.g., radar display along with limited access to non-law enforcement, open source database information). Once access has been approved, all users are required to sign the AMOSS Rules of Behavior, which is tailored after the DHS Rules of Behavior. Any information sharing arrangements involving the transmission of PII must be reviewed and approved by CBP's Office of Chief Counsel, the CBP Privacy Officer, and the DHS Chief Privacy Officer.

Responsible Officials

Tony Crowder
Executive Director
Air and Marine Operations Center (AMOC)

Laurence Castelli
CBP Privacy Officer

Approval Signature

Original signed and on file with the DHS Privacy Office

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security