Transportation Security Administration

TSA MANAGEMENT DIRECTIVE No. 1300.4
REQUEST FOR SECURE FLIGHT DATA

To enhance mission performance, TSA is committed to promoting a culture founded on its values of Integrity, Innovation and Team Spirit.

REVISION: This revised directive supersedes TSA MD 1300.4, *Request for Secure Flight Data*, dated December 24, 2014.

SUMMARY OF CHANGES: Section 7, Procedures, processing request for Secure Flight data has been changed from Secure Flight Branch to Secure Flight Operations Center.

1. **PURPOSE:** This directive provides TSA policy and procedures for responding to requests for Secure Flight Data (SFD) by TSA employees and other agencies. This directive does not restrict the disclosure of SFD initiated by TSA to respond to threats to transportation or national security where disclosure is in accordance with the Privacy Act.

2. **SCOPE:** This directive applies to all requests for SFD by TSA employees, contractors, and other agencies.

3. **AUTHORITIES:**

   A. Aviation and Transportation Security Act of 2001, 49 U.S.C. § 114 *et seq*.

   B. Intelligence Reform and Terrorism Prevention Act of 2004, Section 2012 (codified at 49 U.S.C. § 449030(2))

   C. Privacy Act of 1974, 5 U.S.C. § 552a

   D. Privacy Act of 1974, System of Records; Secure Flight Records

   E. Secure Flight Rule, 49 CFR Part 1560

4. **DEFINITIONS:**

   A. Internal Use: The use of a record by an Internal User.

   B. Internal User: A TSA employee or government contractor who has a need for the record in the performance of his or her official duties.

   C. Law Enforcement Agency: A governmental agency or instrumentality of any jurisdiction within the United States or under the control of the United States authorized by law to conduct civil or criminal law enforcement activities. For purposes of this directive, law enforcement agency includes other components of the U.S. Department of Homeland Security (DHS), and organizations supported by TSA employees on detail, including Joint Terrorism Task Forces.

D. Routine Use: A use published in the Federal Register for a system of records that permits the disclosure of a record in the Secure Flight System of Records. Disclosures made pursuant to Routine Uses must be compatible with the purpose for which the record was initially collected.[1]

E. Secure Flight Data (SFD): Includes both Secure Flight Passenger Data, as defined in Section 4(F) below, as well as passenger prescreening results and analysis.

F. Secure Flight Passenger Data (SFPD): SFPD is information regarding a passenger or non-traveling individual that a covered aircraft operator or covered airport operator transmits to TSA and includes the individual's full name, date of birth, gender, Redress Number, Known Traveler Number, passport information, reservation control number, record sequence number, record type, passenger update indicator (verified identity indicator), and traveler reference number.

5. RESPONSIBILITIES:

A. Assistant Administrators and the Chief Counsel are responsible for:

(1) Educating their employees and contractors on this policy.

(2) Referring requests for SFD to the Office of Intelligence and Analysis (OIA) for processing when required by this directive.

B. Office of Intelligence and Analysis (OIA) is responsible for:

(1) Receiving and processing requests for SFD from TSA employees and other agencies when required by this directive;

(2) Approving SFD disclosure requests from agencies external to TSA with the concurrence of the Chief Counsel and the Privacy Officer or their designees; and

(3) Maintaining an appropriate accounting of all disclosures of SFD to other agencies under this policy.

C. The Office of Chief Counsel (OCC) is responsible for providing timely advice and review of requests for SFD for conformity with this policy and applicable laws, regulations, and DHS policy and procedures.

D. The Privacy Officer is responsible for providing timely advice and review of requests for SFD for conformity with this policy and appropriateness for release.

6. POLICY:

A. The Secure Flight program enhances the security of air travel within the United States and supports the Federal Government's counterterrorism efforts by assisting in the detection of individuals identified on a watch list maintained by the Federal Government who seek to travel

by air. Nothing in this directive is intended to create any substantive or procedural rights, privileges or benefits enforceable in any administrative, civil, or criminal matter.

B. SFD shall not be shared for purposes of ordinary law enforcement or tracking the movement of an individual who is not a potential or confirmed match to a watch list.

C. TSA may disclose information on individuals *who are a match or potential match* to a watch list in accordance with the Privacy Act, such as where the disclosure is internal to TSA to employees who have a need for the information in the performance of their duties, or is pursuant to an existing Routine Use published in the Secure Flight System of Records Notice. Requests for SFD must identify the individual(s); however, bulk or routine programmatic transfer of SFD may be implemented upon approval by the Privacy Office, OCC, and OIA.

D. TSA may disclose information on individuals who *are not a match or potential match* to a watch list only as follows:

(1) To Internal Users for compliance investigations, litigation, match determination inquiries, Federal Air Marshal Service mission coverage planning, operation analysis, screening coordination, Freedom of Information Act (FOIA), and DHS Traveler Redress Inquiry Program (TRIP) requests.

NOTE: *Internal Users may not provide SFD to other law enforcement agencies*, unless approved by the Chief Counsel and Privacy Officer or their respective designees. Requests for SFD must identify the individual(s), unless a flight manifest is requested in response to a specific security threat. Internal Users seeking access to SFD for purposes other than those listed in this subparagraph must follow the procedures in Section 7(B);

(2) To the U.S. Department of Transportation for purposes of investigating a complaint by the individual against an aircraft or airport operator;

(3) To the Terrorist Screening Center, National Targeting Center, or aircraft operators for a match determination inquiry or in response to a Domestic Events Network notification or other event threatening a flight; and

(4) To a law enforcement agency or intelligence agency which has submitted a request pursuant to the procedures in Section 7(C), or pursuant to written arrangement regarding procedures for response to a specific security threat to a flight or exigent threat to life where the procedures are approved by the Privacy Office, OCC, and OIA.

(5) To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, including the World Health Organization, for purposes of assisting such agencies or organizations in preventing exposure to or transmission of communicable or quarantinable disease or for combating other significant public health threats.

E. There may be occasions when the purpose of a request does not demonstrate a nexus to terrorism or a risk to transportation security. Such requests may be considered on a case-by-

case basis where an exigent threat to life or a similar extraordinary circumstance suggests that disclosure is warranted.

Example: A request for SFD for a suspected kidnapper may warrant consideration under the procedures in Section 7(C), where the information could be used to prevent harm to the victim.

7. PROCEDURES:

A. The following requests for SFD will be processed directly by the Secure Flight Operations Center:

(1) Requests by Internal Users for compliance investigations, litigation, match determination inquiries, Federal Air Marshal Service mission coverage planning, operations analysis, FOIA, and screening coordination;

(2) Requests for use by DHS TRIP;

(3) Requests for use by the U.S. Department of Transportation for purposes of investigating a complaint by an individual against an aircraft or airport operator;

(4) Requests for use by the Terrorist Screening Center, National Targeting Center, or aircraft operators for a match determination inquiry or in response to a Domestic Events Network notification or other event threatening a flight; and

(5) To the Centers for Disease Control and Prevention (CDC) or other health agency, or DHS National Operations Center for purposes of assisting in preventing exposure to or transmission of communicable or quarantinable disease or for combating other significant public health threats.

B. Requests for SFD by Internal Users for a use not covered by Section 7(A) will be processed as follows:

(1) Requests will be routed to the Secure Flight Operations Center, (240) 473-1665, or via e-mail to SFOperations@tsa.dhs.gov.

(2) Requests need not be submitted in writing. However, the Internal User making the request must provide the following information;

(a) His or her name;

(b) The information sought;

(c) The purpose for the request; and

(d) Whether any further dissemination of the information is anticipated.

(3) The Secure Flight Operations Center will provide the information, unless it determines, in its sole discretion, that the requestor will use the information for an impermissible purpose;

will disclose the information to an unauthorized person; or will provide the information to an employee of a third party agency, in which case the Secure Flight Operations Center will provide the requestor with instructions for submitting third party agency requests under Section 7(C).

(4) The Secure Flight Operations Center will maintain an accounting of SFD requests made under this policy for compliance and review purposes.

C. Requests for SFD from agencies external to TSA not covered by Section 7(A), including requests pertaining to individuals listed on a watch list, will be processed as follows:

(1) Requests will be routed to the Secure Flight Operations Center, (240) 473-1665, or via e-mail to SFOperations@tsa.dhs.gov.

(2) Requests must be in writing and contain the information described in Attachment A, except requests submitted pursuant to a written arrangement under 6(D)(4) must follow the requirements of the arrangement. If necessary, the requesting agency may classify the request.

(3) The Secure Flight Operations Center will conduct an initial screening of the request, which may include a preliminary search of the Secure Flight System without providing data to the requestor. If there are no potentially responsive records, the Secure Flight Operations Center will inform the requestor and close the request.

(4) If there are records potentially responsive to the request regarding an individual(s) on a watch list, the Secure Flight Operations Center may release the record pursuant to the applicable routine use published in the Secure Flight System of Records Notice. If there are any records potentially responsive to the request regarding an individual(s) NOT on a watch list, the Secure Flight Operations Center will consult with OCC and the Privacy Officer, both of which will make a prompt recommendation on whether the records should be released. If OCC and the Privacy Officer concur that the request has a nexus to transportation or national security and recommend release of the records to the requestor, the recommendations will be presented to the OIA Assistant Administrator for a decision.[2] If OIA, OCC, and/or the Privacy Officer recommend against release, OIA may deny the request, or any of the three offices may recommend forwarding the request to the TSA Administrator for a final determination. OIA will assemble all recommendations for presentation to the TSA Administrator for a decision on release.

(5) Requests determined by OIA, OCC, and/or the Privacy Officer to be unrelated to transportation or national security will be evaluated for extraordinary circumstances that may support disclosure pursuant to 5 U.S.C. § 552a(b)(7). OIA, OCC, and the Privacy Officer will each make a recommendation on release of potentially responsive records. If OIA, OCC, and the Privacy Officer concur that release is warranted, the recommendations will be presented to the OIA Assistant Administrator, who may release the records to the requestor. If OIA, OCC, and/or the Privacy Officer recommend against release, OIA may deny the request or any of the three offices may recommend forwarding the request to the TSA Administrator. OIA will assemble all recommendations for presentation to the TSA

Administrator for a decision on release.

D. TSA response to requests:

(1) Any SFD provided in response to a request under this directive will remain designated Sensitive Security Information (SSI). Further dissemination of SFD provided in response to a request must be approved by TSA in accordance with the SSI regulations, 49 CFR Part 1520.

(2) The Secure Flight Operations Center will maintain an appropriate accounting of all requests for SFD as required by the Privacy Act, 5 U.S.C. § 552a(c)(1), including the date, nature, and purpose of each disclosure made under this policy.

E. Disclosure of SFD for individuals who *are a match or potential match* to a watch list may be accomplished affirmatively in accordance with the Privacy Act, such as where the disclosure is:

(1) Internal to TSA and to TSA employees who have a need for the information in the performance of their duties; or

(2) Pursuant to an existing Routine Use published in the Secure Flight System of Records Notice.

Example: A Federal Security Director may alert the Federal Bureau of Investigation (FBI) to the scheduled travel of a No Fly or Selectee List match so that the FBI may make appropriate operational plans. Such disclosures by TSA do not require a request or use of the process in Section 7(A), (B), or (C) under this directive.

8. APPROVAL AND EFFECTIVE DATE: This policy is approved and effective the date of signature unless otherwise specified.

APPROVAL

Signed March 16, 2015

_____ _____

Joseph C. Salvator
Assistant Administrator
Office of Intelligence and Analysis

Date

EFFECTIVE

_____

Date

Distribution:	Office of Security Operations; Office of Law Enforcement/Federal Air Marshal Service; Office of Chief Counsel; Office of Inspection; Office of Intelligence and Analysis; Office of Global Strategies; Office of Security Policy and Industry Engagement, Office of Civil Rights and Liberties; Ombudsman and Traveler Engagement; Risk Based Security
Point of Contact:	TSA Privacy Office, TSAPrivacy@tsa.dhs.gov

Attachment A

Guidance to Law Enforcement Agencies on Requests for Secure Flight Data

As required by section 4012(a) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), the Transportation Security Administration's (TSA) Secure Flight program matches identifying information of commercial aviation passengers and certain non-travelers against the consolidated and integrated terrorist watch list maintained by the Federal Government. Through Secure Flight, TSA receives information relating to every commercial airline passenger reservation into, out of, over and within the United States. This information is designated Secure Flight Data (SFD).

SFD is protected by the Privacy Act of 1974 and further restricted by TSA policy. TSA may provide SFD to law enforcement agencies as described in the Secure Flight System of Records Notice (SORN) for individuals TSA determines to be a potential or confirmed match to the terrorist watch list. In addition, TSA may also respond to a law enforcement agency's request for SFD on an individual listed on the consolidated and integrated terrorist watch list under the provisions of the Secure Flight SORN.

For individuals <u>not</u> listed on the consolidated and integrated terrorist watch list, TSA will only respond to a written request for SFD by a law enforcement agency when there is a nexus to terrorism, transportation security, or national security. Exceptions to this policy may be granted on a case-by-case basis where an exigent threat to life or a similar extraordinary circumstance suggests that disclosure is warranted. Requests for SFD must conform to the requirements of the Privacy Act (5 U.S.C. § 552a(b)(7)), and must:

1. Be in writing;
2. Specify the particular investigation being conducted;
3. Specify the particular records being sought, including the timeframe and scope of the request;
4. Provide sufficient information to determine whether there is a nexus to terrorism, transportation, or national security, or where an exigent threat to life or a similar extraordinary circumstance suggests that disclosure is warranted; and
5. Be signed by the Chief or other head of a state, local, tribal or territorial law enforcement agency, or an individual no lower than a Unit Chief or equivalent supervisory official.

The following template is intended to assist law enforcement agencies with submitting SFD requests. All requests for SFD are processed by the OIA Headquarters Intelligence Watch. Questions may be directed to Secure Flight, (240) 473-1665, or via e-mail to SFOperations@tsa.dhs.gov.

[PLEASE USE AGENCY LETTERHEAD]

[Requests may include Classified National Security Information. If submitting in a classified format, please comply with all Executive Order 13526 marking requirements.]

Administrator
Transportation Security Administration
601 South 12th Street
Arlington, Virginia 20598

Dear Sir:

The [name of law enforcement agency] is currently investigating the facts and circumstances [nature of the civil or criminal law enforcement inquiry]. This investigation [does/does not] involve [national security, terrorism, and/or transportation security.]

Pursuant to [citation to statutory authority authorizing the agency to conduct the inquiry], this [agency/instrumentality] is responsible for conducting such [civil/criminal] law enforcement activities.

In furtherance of our investigative efforts, we request that the specific records identified below be provided. Only information that is considered minimally necessary for the proper conduct of the inquiry is being sought.

[Identification of records]

To the extent the records are covered by the Privacy Act of 1974, this request is made pursuant to section 552a(b)(7) of title 5, United States Code.

The records furnished will only be used for the sole purpose of the ongoing law enforcement activity and for no other purposes. The information will be protected from unauthorized use or disclosure and will be destroyed when no longer needed for the investigation unless it is retained for evidentiary or other lawful purposes.

If you have any questions, my point of contact for this matter is [name, telephone, e-mail (for classified requests, include secure contact information)].

Sincerely,

[Must be signed by the head of the requesting agency, or a delegated official; include name and title]