4910-9X

DEPARTMENT OF TRANSPORTATION

Office of the Secretary

[Docket No. DOT-OST-2012-0102]

Privacy Act of 1974; Department of Transportation Office of the Secretary – DOT/OST-100 Investigative Record System

AGENCY: Office of the DOT Chief Information Office, Office of the Secretary, DOT.

ACTION: Notice of revised Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Transportation proposes to update and reissue a current Department of Transportation system of records titled, DOT/OST 100 Investigative Record System. This system of records will allow the Department of Transportation Office of the Inspector General to collect and maintain records on individuals who may be complainants, subjects, witnesses, and others who may be identified during the course of an investigation. The records and information collected and maintained in this system are used to document the processing of allegations of violations of criminal, civil, and administrative laws and regulations relating to DOT programs, operations, and employees, as well as contractors and other individuals and entities associated with DOT.

As a result of biennial review of the system, this system of records notice has been updated within the system name, system location, categories of individuals and records in the system, authority for maintenance of the system, purposes, routine uses, as well as storage, retrievability, safeguards, retention and disposal, system manager and address, notification procedure, and record source categories. There will be no change

to the Privacy Act exemptions in place for this system of records. However, the system of records notice as published in 2000 omitted certain exemptions contained in DOT's Privacy Act regulations. The revised system of records notice will correct this error. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. This updated and revised system will be included in the Department of Transportation's inventory of record systems.

DATES: *Effective* August 18, 2012. Written comments should be submitted on or before the effective date. If no comments are received, the proposal will become effective on the above date. If comments are received, the comments will be considered and, where adopted, the documents will be republished with changes.

ADDRESSES: You may submit comments, identified by Docket Number DOT-OST-2012-0102., by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Mail: Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Ave. SE., West Building Ground Floor, Room W12–140, Washington, DC 20590–0001.
- Hand Delivery or Courier: West Building Ground Floor, Room W12–140, 1200 New Jersey Ave. SE., between 9 a.m. and 5 p.m. ET, Monday through Friday, except Federal Holidays.
- Fax: (202) 493–2251.

Instructions: You must include the agency name and docket number DOT-OST-2012-0102.

All comments received will be posted without change to http://www.regulations.gov, including any personal information provided. Anyone is able to search the electronic form of all comments received in any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.).

Docket: For access to the docket to read background documents or comments received, go to *http://www.regulations.gov* or to the street address listed above. Follow the online instructions for accessing the docket.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Seth B. Kaufman, Department of Transportation, Office of Inspector General, Seventh Floor, J-3, 1200 New Jersey Ave. SE, Washington, D.C. 20590; or by facsimile (202) 366-1975. For privacy issues please contact: Claire W. Barrett, Departmental Chief Privacy Officer, Privacy Office, Department of Transportation, Washington, D.C. 20590; privacy@dot.gov; or (202) 527-3284.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. §552a, the Department of Transportation (DOT) Office of the Secretary proposes to update and reissue a previously published DOT system of records titled DOT/OST 100 Investigative Record System. This system of records will allow the Department of Transportation Office of the Inspector General to collect and maintain records on individuals who may be complainants, subjects, witnesses, and others who may be identified during the course of an investigation. As noted above, the primary intent of the revision is to add routine

uses to this system. We also seek to update and clarify other parts of the system of records notice (SORN) in part to reflect changes to the OIG organization and programs since its last publication in 2000.

The DOT Inspector General is responsible for conducting and supervising independent and objective audits, inspections, and investigations of the programs and operations of DOT. OIG promotes economy, efficiency, and effectiveness within the Department and prevents and detects fraud, waste, and abuse in its programs and operations. OIG's Office of Investigations investigates allegations of criminal, civil, and administrative misconduct involving DOT employees, contractors, grantees, and Departmental programs and activities. This includes investigating for violations of criminal laws by entities regulated by DOT, regardless of whether they receive Federal funds. These investigations can result in criminal prosecutions, fines, civil monetary penalties, and administrative sanctions.

The DOT/OST 100 Investigative Record System system of records assists the OIG with receiving and processing allegations of violation of criminal, civil, and administrative laws and regulations relating to DOT employees, contractors, grantees, regulated persons, and other individuals and entities associated with DOT. The system includes both paper investigative files and OIG's electronic case management and tracking information system which also generates reports. The case management system allows OIG to manage information provided during the course of its investigations, and, in the process, to facilitate its management of investigations and investigative resources. Through this system, OIG can create a record showing disposition of allegations; track actions taken by management regarding misconduct; track legal

actions taken following referrals to the U.S. Department of Justice for prosecution or civil action; provide a system for creating and reporting statistical information; and track government property and other resources used in investigative activities.

This SORN makes several changes to the existing system of records. It amends the system name, system locations, purposes, routine uses, as well as storage, retrievability, safeguards, retention and disposal, system manager and address, notification procedure, and record source categories.

OIG's field office locations have undergone changes since this SORN was last updated. The proposed SORN will not list the location of specific field offices to avoid the need to update the SORN as locations of OIG field offices change. OIG's field offices are available on the OIG website. Accordingly, listing of individual regional offices in the SORN is not necessary.

The categories of individuals and records covered by the system have been revised to more clearly reflect OIG practice. The revision does not make any substantive change in longstanding OIG practice. Accordingly, there are no privacy impacts associated with these changes.

The categories of individuals covered by the previously published SORN include present and former DOT employees, DOT contractors and employees as well as grantees, sub-grantees, contractors, subcontractors and their employees and recipients of DOT monies, and other individuals or incidents subject to investigation within the purview of the Inspector General Act. In the revised SORN, we clarify that the system includes complainants, individuals alleged to have been involved in wrongdoing, individuals identified as possibly relevant to the investigation or who are contacted by

OIG during the investigation; and DOT OIG investigative personnel. The revised SORN does not reflect any expansion of the categories of individuals covered by the system.

We are also clarifying the record categories in the system. The previously published SORN describes the categories as the results of investigations. A report of investigation by nature contains many types of personal information. The SORN that has been in place does not, however, describe with particularity the types of personal information that may be contained in this system. The revised SORN gives more information about the categories of records that OIG actually maintains in this system.

The authority for the maintenance of the system has been amended to include additional authority. In 1999, the Motor Carrier Safety Improvement Act, Public Law 106-159, Section 228, clarified that OIG's statutory authority of the Inspector General of the Department of Transportation includes authority to conduct, pursuant to Federal criminal statutes, investigations of allegations that a person or entity has engaged in fraudulent or other criminal activity relating to the programs and operations of the Department or its operating administrations. It also provided that the authority to conduct these investigations extends to any person or entity subject to the laws and regulations of the Department or its operating administrations, whether or not they are recipients of funds from the Department or its operating administrations. Although this law, later codified at 49 U.S.C. Section 354, was intended to be a clarification of OIG's existing statutory authority, we believe it appropriate to cite this statute in the authority section of the SORN.

The purposes of the system have been revised to more clearly identify OIG practices. The existing version states that the purposes of the system are to "[d]ocument the

administration of investigations and inquiries conducted under of the Inspector General Act of 1978." The Inspector General Act provides authority for OIG to conduct a number of different types of investigations. The proposed version contains more specific purposes for the system, but makes no substantive changes.

The routine uses have been updated to reflect current practices with the OIG community. New routine uses include disclosure of records in this system of records to the media and the public when the public interest requires and when such disclosure does not constitute an unwarranted invasion of privacy. The routine use for public and media disclosures is to fulfill the mission of the Inspector General to deter and detect waste, fraud, abuse, and violations of law. It could be used for media releases for purposes such as helping to locate suspects or publicizing particular cases to maximize their deterrent value. These types of disclosures will require the approval of OIG counsel after review of the privacy interests involved and the need for public disclosure. We also propose a routine use for disclosure to individuals who are in danger or in situations involving an imminent danger of death or physical harm. The new routine uses also include disclosure of records to recipients of Federal funds and entities regulated by DOT when such disclosure is for the purpose of recovering DOT funds or enabling disciplinary or corrective action. This routine use would help employers to take appropriate action with respect to their employees, contractors, subcontractors, and others who have committed violations of law, agency policy, or other misconduct. We also seek a routine use for disclosures to other Federal agencies the purpose of oversight, such as peer reviews of the OIG Office of Investigations. Accordingly, any

effects on privacy interests due to these routine uses are justified, appropriate, and in the public interest.

The revised SORN also updates storage, retrievability, and safeguards to reflect modern standards. For instance, the storage and retrievability sections explicitly reference the use of electronic records. The access controls on electronic records include two-factor authentication, password protection features, and network authentication. These new access controls increase the privacy protections afforded to these records.

The retention and disposal section reflects the National Archives and Records Administration (NARA)-approved disposition schedule for these records which was approved since the last update to the SORN.

The system manager and address is being changed to reflect a title change for the head of the OIG Office of Investigations. The previously published SORN lists the system manager as the Assistant Inspector General for Investigations. The duties, functions, and authority for the Principal Assistant Inspector General for Investigations are in all material respects the same as those formerly held by the Assistant Inspector General for Investigations. In addition, the address of the system manager is being updated to reflect a relocation of the Department of Transportation to a new building within the District of Columbia. Accordingly, there are no substantive changes to these sections.

The record source categories more clearly state the types of sources for records that are obtained for this system. The previously published SORN states that record sources are obtained from interviews, review of records and other authorized investigative techniques. The previously published SORN emphasizes the methods by which OIG

obtains records. In this revision, we seek to clarify the types of individuals from which OIG obtains records. These changes do not reflect any substantive changes.

Consistent with DOT's information sharing mission, information stored in the DOT/OST 100 Investigative Record System system of records may be shared with appropriate Federal, State, local, tribal, foreign, or international government agencies. This sharing will only take place after OIG determines that the receiving agency has a need to know the information to carry out law enforcement or other functions consistent with the routine uses set forth in this system of records notice.

There will be no change to the Privacy Act exemptions previously established for this system of records. The Appendix to Part 10, Title 49, Code of Federal Regulations, contains the Privacy Act exemptions for all DOT systems of records. Paragraph D of Part II of the Appendix provides that those portions of DOT/OST 100 consisting of investigatory material compiled for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, or access to classified information or used to determine potential for promotion in the armed services, are exempt from sections (c)(3) (Accounting of Certain Disclosures), (d) (Access to Records), (e)(4) (G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) of 5 U.S.C. 552a to the extent that disclosure of such material would reveal the identity of a source who provided information to the Government under an express or, prior to September 27, 1975, an implied promise of confidentiality (5 U.S.C. 552a(k) (5) and (7)). These exemptions under (k)(5) and (k)(7) appear to have been inadvertently omitted when DOT/OST 100 was last published in 2000. The revised SORN corrects

this error and harmonizes the SORN with these exemptions that have been codified in Federal regulations for many years.

The exemption for records used to determine promotion in the armed forces potential is needed for records relating to the United States Coast Guard (USCG). USCG was part of DOT until its transfer to the Department of Homeland Security in March 2003. OST/DOT 100 contains records of investigations relating to USCG programs and operations. Until these records reach their end of the retention period, OIG has need of this exemption. After the retention period is over, OIG will re-assess its need for this exemption.

II. Privacy Act

The Privacy Act (5 U.S.C. 552a) governs the means by which the Federal Government collects, maintains, and uses personally identifiable information (PII) in a System of Records. A ‘‘System of Records’’ is a group of any records under the control of a Federal agency from which information about individuals is retrieved by name or other personal identifier. The Privacy Act requires each agency to publish in the **Federal Register** a System of Records notice (SORN) identifying and describing each System of Records the agency maintains, including the purposes for which the agency uses PII in the system, the routine uses for which the agency discloses such information outside the agency, and how individuals to whom a Privacy Act record pertains can exercise their rights under the Privacy Act (e.g., to determine if the system contains information about them and to contest inaccurate information).

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

SYSTEM OF RECORDS:

Department of Transportation (DOT)/OST-100

SYSTEM NAME:

Department of Transportation/Office of the Inspector General– 100 Investigative Record System

SECURITY CLASSIFICATION:

Unclassified - sensitive.

SYSTEM LOCATION:

Records are maintained at the DOT OIG Headquarters in Washington, D.C., and in DOT OIG field offices nationwide. Records are also maintained by Federal Records Centers.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals filing complaints of criminal, civil, or administrative violations, including, but not limited to, fraud, waste, or mismanagement; individuals alleged to have been involved in such violations; individuals identified as having been adversely affected by matters investigated by the OIG; individuals who have been identified as possibly relevant to, or who are contacted as part of, an OIG investigation, including: (A) current and former employees of the DOT, other Federal agencies, and DOT contractors, grantees, and persons whose association with current and former employees relate to alleged violations under investigation; and, (B) witnesses, complainants, confidential informants, suspects, defendants, or parties who have been identified by the DOT OIG, other DOT components, other agencies, or members of the general public in connection

with authorized OIG functions; and DOT OIG employees performing investigative functions.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system include:

- Investigative agent name and contact information
- Individual's name and aliases;
- Date of birth;
- Social Security Number;
- Telephone and cell phone numbers;
- Physical and mailing addresses;
- Electronic mail addresses;
- Physical description;
- Citizenship;
- Photographs;
- Job title, employment position, and other employment data;
- Medical history;
- Any other personal information relevant to the subject matter of an OIG investigation;
- Investigative files containing complaints and allegations, witness statements; transcripts of electronic monitoring; subpoenas and legal opinions and advice; reports of investigation; reports of criminal, civil, and administrative actions taken as a result of the investigation; and other relevant evidence;
- Property receipts establishing chain of custody of evidence.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The Inspector General Act of 1978, as amended, and 49 U.S.C. § 354.

PURPOSE(S):

The records and information collected and maintained in this system are used to document the processing of allegations of violations of criminal, civil, and administrative laws and regulations relating to DOT programs, operations, and employees, as well as contractors and other individuals and entities associated with DOT; monitor case assignments, status, disposition, and results; manage investigations and information provided during the course of such investigations; track actions taken by management regarding misconduct and other allegations; track legal actions taken following referrals to the Department of Justice for prosecution or litigation; create and report statistical information; and manage property records establishing chain of custody of evidence.

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

1. To other Federal, State, local, or foreign agencies or administrations, and licensing and professional discipline authorities, having interest or jurisdiction in the matter.
2. To third parties in the course of an investigation, when necessary to obtain pertinent information.

3. To any person when disclosure of the record is needed to enable the recipient of the record to take action to recover money or property of DOT, when such recovery will accrue to the benefit of the United States, or when disclosure of the record is needed to enable the recipient of the record to take appropriate disciplinary or corrective action to maintain the integrity of DOT programs or operations.
4. To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.
5. To media and the public when the public interest requires, unless it is determined by OIG counsel that release of specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.
6. To an individual or individuals who are in danger or in situations involving an imminent danger of death or physical injury.
7. To other agencies and the Council of Inspectors General on Integrity and Efficiency (CIGIE) for purposes of conducting and reviewing peer reviews of the OIG to ensure adequate internal safeguards and management procedures exist or to ensure that standards applicable to Government audits, investigations, or other agency activities are applied and followed.

8. For other routine uses of the information, applicable to all DOT Privacy Act systems of Records, see ‘‘Prefatory Statement of General Routine Uses’’ (available at *http://www.dot.gov/privacy/privacyactnotices*).

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETRAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records in this system are stored electronically and/or on paper in secure facilities. Electronic records may be stored on magnetic disc, tape, digital media, and CD-ROM.

RETRIEVABLITY:

Paper media are retrieved alphabetically by name of subject or complainant, by case number, and/or by special agent name and/or employee identifying number. Electronic media are retrieved by the name or identifying number for a complainant, subject, victim, or witness; by case number; by special agent name or other personal identifier; or by field office designation.

SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DOT 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 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.

Paper files are stored in file cabinets in a locked file room to which only authorized personnel are provided access, on a need-to-know basis.

RETENTION AND DISPOSAL:

Records will be retained and disposed in accordance with National Archives and Records Administration (NARA) records disposition schedule for OIG Investigative Case Files (N1-398-02-1, March 3, 2002).

Files containing information or allegations which old, are of an investigative nature but do not relate to a specific investigation such as anonymous or vague allegations not warranting an investigation, matters referred to constituents or other agencies for handling, and support files providing general information which may prove useful in Inspector General investigations are destroyed when 5 years old.

All other investigative case files (except those that are unusually significant for documenting major violations of criminal law or ethical standards by agency officials or others) are placed in inactive files when case is closed. The cutoff for inactive files occurs at the end of fiscal year. These files are destroyed ten years after cut off. The disposition of significant cases (i.e., those that result in national media attention, Congressional investigations and/or substantive changes in agency policy or procedures) will be determined by NARA and will be scheduled separately.

SYSTEM MANAGER(S) AND ADDRESS:

The System Manager is the Principal Assistant Inspector General for Investigations, DOT OIG, Seventh Floor, JI-1, 1200 New Jersey Ave. SE, Washington, D.C. 20590.

NOTIFICATION PROCEDURE:

The Secretary of Transportation has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, the Office of Inspector General will consider individual requests to determine whether or not information may be released.

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 DOT or OIG FOIA Officer whose contact information can be found at *http://www.dot.gov/foia* under "Contact Us." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Departmental Freedom of Information Act Office, U.S. Department of Transportation, Room W94-122, 1200 New Jersey Ave., SE., Washington, D.C. 20590, ATTN: FOIA request.

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 49 CFR Part 10. 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 Freedom of Information Act Officer, *http://www.dot.gov/foia* or 202.366.4542. In addition you should provide the following:

- An explanation of 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;
- Provide any other information that will help the FOIA staff determine which DOT component agency may have responsive records; and

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 are obtained from sources including, but not limited to, the individual record subjects; DOT employees, grantees, and contractors; employees of Federal, State, local, and foreign agencies; and other persons and entities.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Pursuant to 5 U.S.C. 552a(j)(2), this system is exempt from the following provisions of the Privacy Act: 5 U.S.C. 552a (c)(3)-(4); (d); (e)(1)-(3); (e)(4)(G)-(I); (e)(5); (e)(8); and (f)-(g).

Pursuant to 5 U.S.C. 552a(k)(1), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a(c)(3); (d); (e)(4)(G)-(I) and (f).

Pursuant to 5 U.S.C. 552a(k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a(c)(3) and (d).

Pursuant to 5 U.S.C. 552a(k)(5) and (k)(7), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a (c)(3); (d); (e)(4)(G)-(I); and (f).

Issued in Washington, DC on July 19, 2012

Claire W. Barrett

Departmental Chief Privacy Officer

[FR Doc. 2012-17696 Filed 07/19/2012 at 8:45 am; Publication Date: 07/20/2012]