U.S. Department of Transportation

Privacy Impact Assessment

Office of the Secretary (OST)

Personnel Enterprise Security System (PSES)

Responsible Official

Linda Guier
Associate Director, Personnel Security
Office of Security, Personnel Security and ID Media
202.366.4677
SEAD3@dot.gov

Reviewing Official

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
202.366.8135
privacy@dot.gov

CLAIRE W BARRETT Digitally signed by CLAIRE W BARRETT
Date: 2020.09.22 15:12:20 -04'00'

Executive Summary

The Department of Transportation's (DOT) Office of Security, Personnel Security Division (M-40), is responsible for conducting and managing background investigations mandated by Executive Order (E.O.)12968 as amended, "Access to Classified Information," for all federal and contract employees to obtain a badge, credential, or a national security clearance. In support of this function, DOT procured and operates the Personnel Security Enterprise System (PSES), which automates the personnel security functions through a suite of integrated workflow and case management modules. This Privacy Impact Assessment (PIA) was conducted because PSES collects and maintains personally identifiable information (PII) on individuals employed by, or seeking employment with, DOT.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*

[1] Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

The Personnel Security Enterprise System (PSES) is a commercial off-the-shelf (COTS) solution that supports the entire lifecycle of DOT's personnel and administrative security cases and enterprise security functions. PSES is used to track and manage the information and records necessary to conduct employee background investigations and determine eligibility for clearances. The system captures data related to all aspects of pre-appointments, suitability and fitness determinations, security clearance processing, briefings, foreign travel, foreign contacts, procurement processes for classified contracts, documentation for DOT employees who attend classified briefings outside of DOT, and non-DOT individuals attending classified meetings at DOT. Additionally, the system allows the Department to collect metrics and report on operational performance, as mandated, to Office of Personnel Management (OPM) and Director of National Intelligence (ODNI) for full operational compliance with the new Federal Investigative Standards.

The Office of the Secretary (OST) and DOT Operating Administrations (OA)[2] except for the Federal Aviation Administration (FAA)[3] and the Office of the Inspector General (OIG)[4] use PSES for the entire security lifecycle process.

Before any information is entered into PSES, the prospective employee/contractor must complete the proper paperwork, such as the electronic personnel security questionnaire (e-QIP) and other forms as described further in this document. The employee/contractor is provided with the documents by the Human Resources specialist for federal employees or the Contract Officer Representative (COR) for contractors. These documents are submitted to the Personnel Security Office and the data is entered into the system to initiate a record.

[2] Operating Administrations within DOT include FAA, FRA, FTA, MARAD, NHTSA, PHMSA, and OST.

[3] The FAA has delegated authority to manage its own personnel security program. As such, FAA employees and contractors are not in the PSES system. Appendix B provides further information on FAA in relation to PSES.

[4] The OIG operates an independent IT network and cannot directly access PSES. Information on OIG employee and contractor cases are uploaded into PSES by M-40 staff who work with OIG to update and adjudicate the records. OIG provides M-40 the paperwork required for an investigation, and M-40 enters the information into PSES. For completed investigations returned to PSES from DCSA, M-40 provides a password protected PDF copy to OIG's Suitability Adjudicator to adjudicate the investigation for a final determination. OIG then sends the documents used to make that final determination back to M-40 for upload into PSES.

To fulfill the purpose of the system, PSES collects information from members of the public; citizens and Legal Permanent Residents (LPR); visitors to DOT for official business; members of the DOT federal workforce; and members of the DOT contract workforce. PSES collects the following PII: name, date of birth (DOB), social security number (SSN), home address, home phone number, investigative and employment history, reports of investigations, records of security and suitability determinations, records of access authorizations granted, documentation of security briefings/debriefings received, individual notifications of business or personal foreign travel, records of security violations, and applications and issuance of official passports and visas.

DOT's PSES configuration does not include all capabilities available in the COTS product. This PIA describes only the PSES modules and capabilities used by the DOT: Personnel Security, Classified Visit Request, Contract DD-254, and Information (document) Security. This PIA also addresses the planned inclusion of the Foreign National Security Executive Agent Directive (SEAD) 3 module.

- **Personnel Security (PerSec)** - Federal policy requires that background investigations are conducted on all federal employees (applicants for federal employment) and contractors who will work on DOT contracts. The PerSec module tracks the personnel security processes and is the foundational module containing the core PII on each employee, employee on detail, contractor and applicant at DOT. The other modules within the system use the information in the PerSec module to validate if an individual is an active DOT employee or contractor, or to validate national security clearance and level of clearance. The processes are as follows:
  - Pre-appointment process - The purpose of this process is to ensure the agency is only spending money on investigations for viable applicants, employees, and contractors. The process includes the review of forms (completed by the applicant/employee or contractor) after a tentative selection is made but before an entry on duty (EOD) date is established, to determine if the candidate can qualify for an HSPD 12 PIV card before the completion of the full background investigation.
  - Suitability process - This is the process where applicants are vetted to determine if they are suitable for federal employment. PSES manages two types of suitability decisions: fitness and national security clearances. All employees must receive a favorable suitability adjudication of a background investigation conducted by the DCSA. The information used to support the investigation process is provided during the pre-appointment phase.
  - Fitness process - Fitness refers to the adjudicative decision made about the fitness/suitability of contractor to perform work on a federal contract supporting the DOT. The system is used to track the fitness/suitability adjudication process and outcome including correspondence with the subject individual used to explain, mitigate, or refute any concerning information developed through interviews or record reviews conducted during the background investigation.

- National Security Clearance - The need for an individual to obtain a national security clearance is determined outside of the suitability process and applies to federal employees only. PSES is used to track the application of the National Security Adjudicative Guidelines, and any correspondence with the subject to explain, mitigate, or refute concerns that were identified during the investigation. PSES also tracks the final determination and indoctrination briefing required for access to classified information.
- Passport and Visa Process – PSES tracks when an employee requests an official passport to travel overseas on official business. The information included is the passport number, date issued, date of expiration, date returned and reason returned. Travel to certain countries requires a visa and PSES tracks all visa requests for official travel to include visa number, date requested, date received, and dates the visa is valid. The system facilities the Department of State (DOS) requirement that individuals return Official Passports to DOS when no longer required or no longer a part of the agency.

PSES also manages the entire step by step process for national security clearance suspensions, clearance reinstatement, clearance denials and clearance revocations. This includes capturing all documents required for presenting to individuals for due process communication, and responses provided by that individual in their defense including appeals presented to the Merit Systems Protection Board.

- **Classified Visit Request** – This module allows the Personnel Security Office to track DOT employees who need to attend National Security classified meetings outside of DOT, as well as visitors who need to attend classified meetings at DOT. Individuals attending classified meetings must have the appropriate minimum clearance on record at DOT before being authorized to attend. Individuals who are not DOT employees must have their clearance passed to DOT by their sponsoring agency to attend classified meetings at DOT. The module documents information on the clearance passed for the classified event, the date the event(s) are held, and personnel/sponsor involved. This module only links a DOT Host person (sponsor) to the visitor's (group/person) clearance level that was passed to DOT by their agency for them to attend a classified briefing/ meeting/ event at DOT. DOT Hosts provide details on the meeting dates and times to personnel security to assist in validating the clearance access of those planning to attend meetings at DOT. PII information on visiting attendees is usually provided by the visitor's agency's Personnel Security Office, and the PII is limited and protected. Occasionally this information is validated from databases outside of PSES, and made available for staff to look up.

  DOT employees attending classified meetings at a non-DOT agency must provide meeting details (location, agency, POC contact information, event type, dates and time and level of classified being discussed) to the Personnel Security office. M-40 generates a memo in PerSec that includes the individual's full name, date of last investigation, date of adjudication, and agency that conducted the investigation and level of clearance. The memo is securely transmitted to the hosting agency for their determination as to whether the individual should be permitted to attend the meeting. The Classified Visit Request module tracks when the information was received from the meeting attendee, when the information was transmitted, and when confirmation received as well as the point-of-contact contact information.

- **Contract DD-254** - This module is used by PerSec to document the physical security, information (document) security, and personnel security requirements that a vendor must follow to support a classified contract with DOT. It is required to ensure individual contractors are cleared by DCSA before working on a contract that requires access to national security information. The process involves the Department of Defense (DoD) and is mandated by E.O. 12829, National Industrial Security Program (NISP), and follows procedures in the NISP Manual DOD 5220.22-M as amended.

  The DD-254 module uses names to identify points of contact who will be associated on classified contracts for the Department, but not on contractors; information on individual contractors is stored in the PerSec module.

- **Information Security** – This module is used to track and inventory all DOT safes with classified information holdings. It is also used to assign the responsibility to oversee the protection of the container, as well as the classified documents inside, to only those allowed access to classified information and the need-to-know. Safes cannot be assigned to individuals who do not have an adjudicated clearance. M-40 staff conducting safe inspections use the Information Security module to identify the location of DOT safes and conduct inventories as well as ensure that there is a valid POC responsible the safe, combinations are changed as prescribed in federal regulations, and removal of safes as warranted. This module contains only the name of the POC for each safe.

- **Foreign National SEAD 3** – This module allows individuals to self-report foreign travel or major life changes as specified in the SEAD 3 Directive issued by ODNI. Templates guide individuals through SEAD-3 prescribed questions and responses in each reporting category. Submissions are digitally signed automatically saved into the PerSec Module security record. An adjudicator reviews the SEAD 3 reports to determine if there is any further action necessary per the SEAD-3 policy guidelines.

PSES also facilitates management oversight to ensure data integrity and adherence to all applicable federal regulations and policies. Supervisors may produce reports and compile metrics, improving the efficacy and efficiency of M-40 operations. PSES also ensures that the processing of all mandatory Periodic Reinvestigations (PRs) occur when federally mandated, and that timelines in each individual record are met. PSES follows federal guidelines to begin the continuous evaluation process conforming to SEAD 6 requirements that will eventually replace the PR process.

PSES is integrated with several internal and external systems. Internally, PSES interfaces with DOT's Card Management System used to issue HSPD-12 compliant personal identity verification (PIV) cards and temporary badges. The system also allows M-40 staff to determine if an investigation is pending with the Office of Personnel Management (OPM) or has been completed before the HSPD-12 PIV badge is issued.

PSES is also integrated with the Office of Human Resource Management's Federal Personnel Payroll System (FPPS) which shares new employee's information such as: position, work location, grade, title, PII, etc. with PSES. PSES shares the completed background investigation back to FPPS such as the type of investigation completed, the date of the investigation, the date adjudicated, and the clearance level grated if appropriate.

Externally, PSES is integrated with the Department of Defense's (DoD) personnel investigations systems. The system supports forms completion, electronic delivery of investigations, and the uploading of required adjudicative decisions on individual's background investigation allowing for full reciprocity of investigations among federal agencies. DoD is authorized under E.O. 13869 Transferring Responsibility for Background Investigations to the Department of Defense, Signed April 29, 2019 to Conduct background investigations that were previously conducted by the National Background Investigation Bureau (NBIB) under the Office of Personnel Management (OPM).

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[5]*, sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*[6]*.*

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures,

[5] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf

[6] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

Records in PSES are retrieved by personal identifier associated with an individual and are protected under the Privacy Act. Records covering the primary purpose of the system maintained in PSES are managed in accordance with the system of record notice (SORN) DOT/OST 035 - Personnel Security Record System - 65 FR 19553 - April 11, 2000. DOT/OST 035 claims exemptions - "Information compiled solely for the purpose of determining suitability, eligibility, or qualification for federal civilian employment or access to classified information may be exempted from the access provisions pursuant to 5 U.S.C. 552a(j)(2), (k)(1) and/or (5)." Please see DOT/OST 35 Privacy Act Exemptions, Final Rule – 80 FR 32039, June 5, 2015.

The SORN covering the Visit Request module is: DOT/OST 046 - Visit Control Records System - 65 FR 19555 - April 11, 2000.

As required by the Privacy Act of 1974, a Privacy Act Statement informing applicants of the Department's privacy practices regarding collection, use, sharing, safeguarding, maintenance, and disposal of PII is included on all applicable paper and web-based forms.

Several forms used to collect information stored in PSES are approved by the Office of Personnel Management (OPM). OPM has published a government-wide Privacy Act System of Records Notice (SORN), OPM/GOVT 1 – General Personnel Records (71 FR 35342, June 18, 2006) and the forms used by DOT include appropriate Privacy Act notices for OPM/GOVT-1 (https://www.opm.gov/forms/standard-forms/) (see Appendix A). The DOT maintains copies of these records consistent with guidance issued by OPM.

The publication of this PIA further demonstrates DOT's commitment to provide appropriate transparency into PSES. Information on the Department's privacy program may be found at www.transportation.gov/privacy.

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

PSES performs data validation on information stored in the system by comparing information received from FPPS and the DoD[7]. If there is a discrepancy in between the data sets, the Personnel Security office will receive an error report.

Individuals are offered the opportunity to address any variance in the PII presented by the investigative service provider (DCSA) during the subject interview portion of the investigation. Subject can also provide the Personnel Security office copies of any official name change or other legal document that modifies the PII information PerSec has in the PSES system.

Individuals with records in PSES also have the opportunity to validate data or correct a portion of their information when they receive their PIV card. Individuals are required to validate their name, organization, and employment status when receiving their PIV card. If the information is incorrect, the PIV card will not be issued until the cause of the discrepancy is identified and corrected.

Under the provisions of the Privacy Act, individuals may request searches of agency records to determine if any added records pertain to them. Individuals wishing to know if their records appear in this system may inquire in person or in writing to:

Claire W. Barrett
Departmental Privacy Officer
1200 New Jersey Ave., SE
E31-312
Washington, DC 20590
Email: privacy@dot.gov
Fax: (202) 366-7024

Department policy requires the inquiry to include the name of the individual, mailing address, phone number or email address, a description of the records sought, and if possible, the location of the records.

Privacy Act requests for records covered by system of records notices not published by the Department will be coordinated with the appropriate customer privacy official and acted upon accordingly.

Additional information about the Department's privacy program may be found at https://www.transportation.gov/privacy-program. Individuals may also contact the DOT Chief Privacy Officer at privacy@dot.gov.

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which its collects, uses, maintains, or disseminates PII.

[7] See Appendix B for more information.

PSES collects the following PII and information about individuals: name, date of birth (DOB), social security number (SSN), home address, home phone number, investigative and employment history, reports of investigations, records of security and suitability determinations, records of access authorizations granted, documentation of security briefings/debriefings received, individual notifications of business or personal foreign travel, records of security violations, as well as applications and issuance of official passports and visas.

The Department has an obligation to conduct background investigations for the purposes of issuing HSPD-12 compliant PIV cards, establishing suitability/fitness, or to grant a national security clearance for access to classified information. The authorities to conduct and maintain PII these investigations are in the following regulations:

- Executive Order 12829 National Industrial Security Program, January 6, 1993, as amended
- Executive Order 12968, Access to Classified Information, August 2, 1995, as amended
- Executive Order 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, June 30, 2008
- Executive Order 13764, Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters, January 17, 2017
- Memorandum from the Director, Office of Personnel Management, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12", July 31, 2008
- Security Executive Agent Directive 3 (SEAD 3), Reporting Requirements for Personnel with Access to Classified Information or Who Hold A Sensitive Position, June 12, 2017
- Security Executive Agent Directive 6 (SEAD 6), Continuous Evaluation, January 12, 2018
- Security Executive Agent Directive 7 (SEAD 7), Reciprocity of Background Investigations and National Security Adjudications, November 9, 2018
- Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004
- National Industrial Security Program Operating Manual DOD 5220.22-M, as amended on May 18, 2016

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. DOT should retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

M-40 manages risk by collecting only the PII relevant and necessary to conduct and manage background investigations. The PerSec Module collects the primary PII for the processing of the background investigations and verifying identities for HSPD-12 PIV card issuance. It collects the minimum amount of information required to identify the person to which the information belongs. This data is retained per General Records schedules listed below. The Visit Request Module is used to send DOT staff national security clearances when individuals attend a classified meeting at another agency. Individuals make the request for the information to be sent to the host agency. This module does not store PII, it only maintains a record that a visit request was sent on subject's behalf.

The DD-254 module uses names to identify points of contact to who will be associated on classified contracts for the Department. This document that is produced by the system lays out all the necessary security protocols relevant for each classified contract the Department procures. Once the contract closes, only basic information identifying the actual company, not individuals, is maintained to show that there was a formal security process in place.

The Information Security Module uses only a person's name that is assigned a safe or classified documents, and only connects the two when a person holding national security is debriefed, after which they are no longer able to be assigned a classified safe or classified documents.

PerSec records are retained in accordance with NARA's General Records Schedule -5.6: Security Records.

- GRS 5.6 - 170 Personnel suitability and eligibility investigative reports: Destroy in accordance with the investigating agency instruction (DAA-GRS-2017-0006-0022).
- GRS 5.6 - 180-181 Personnel security and access clearance records. Records of people not issued clearances. Includes case files of applicants not hired: Destroy 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use (DAA-GRS-2017-0006-0024). Records of people issued clearances: Destroy 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use (DAA-GRS-2017-0006-0025).

The PerSec Module tracks all official passports and visas processed for DOT employees who travel overseas on official duty. Records pertaining to official passports and visas are held in accordance with GRS 2.2, items 90-92, Employee Management Records, items 90-92.

- GRS 2.2 – 90 Application records. Records related to administering the application or renewal of official passports and visas, including: copies of passport and visa applications, passport and visa requests, special invitation letters, visa authorization numbers, courier receipts and copies of travel authorizations. Destroy when 3 years old or upon employee separation or transfer, whichever is sooner; but longer retention is authorized if required for business use (DAA-GRS-2017-0007-0013).
- GRS 2.2 – 91 Official passport registers. Registers and lists of agency personnel who have official passports. Destroy when superseded or obsolete (DAA-GRS-2017-0007-0014).
- GRS 2.2 – 92 Official passports of transferred or separated agency personnel. Transfer to new agency or return to the Department of State upon expiration or upon separation of the employee.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

PSES supports the entire lifecycle of DOT's personnel and administrative security cases and enterprise security functions. It is used to track and manage the information and records necessary to conduct employee background investigations and issue clearances. PII collected in PSES is used for the express purposes detailed within this PIA.

PSES maintains records in accordance with DOT/OST 035, Personnel Security Record System and DOT/OST 046, Visit Control Records System.

Records covered under DOT/OST 35 are used to make suitability determinations for employment or retention in government service, assignment to sensitive duty positions and access to classified information. DOT/OST 35 includes the following purposes for collecting, maintaining, and s sharing of Privacy Act records:

- Used by Departmental personnel security representatives, including contractor personnel, for making security determinations and granting access authorizations, by Departmental personnel management officials for making suitability determinations, by representatives of other federal agencies with which the individual is seeking employment, and by federal agencies conducting official inquiries to the extent that the information is relevant and necessary to the requesting agency's inquiry, and by Departmental officials, to the extent necessary, to identify the individual to sources from whom information is requested for any of the foregoing purposes to inform the source of the nature and purpose of the request and to indicate the type of information requested.

DOT/OST 046 includes the following purposes for collecting, maintaining, and sharing of Privacy Act records:

- Confirming to the proper authorities the security clearance for individuals requiring access to classified information; identifying individuals authorized to be present in DOT facilities.

The Department has also published 14 additional routine uses applicable to all DOT Privacy Act systems of records, including records maintained under DOT/OST-035 and DOT/OST-046. The routine uses are published in the Federal Register at 75 FR 82132, December 29, 2010 and 77 FR 42796, July 20, 2012, under "Prefatory Statement of General Routine Uses" available at http://www.transportation.gove/privacy/privacynotices).

PSES also maintains records in accordance with OPM/GOVT-1 - General Personnel Records which includes the following specific routine use permitting the sharing of Privacy Act records:

The Department discloses PSES records only to those individuals certified by their Agencies as being properly investigated and with the need-to-know the PII for compliance with reciprocity per Office of Management and Budget Memorandum, Reciprocal Recognition of Existing Personnel Security Clearances, December 12, 2005. Additional uses of PSES information is documented in Appendix B.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

All PSES system modules included embedded quality control and accountability features. For example, the system has data field checks as part of the established business rules for the system - number fields only except numbers, alphabet fields only accept alphabets, users cannot proceed to step three if step two is not complete, etc. The system utilizes an audit device to check the integrity of files to ensure that there has not been any malicious activity by means of installing or altering files. In the event of malicious code detection, the applicable code/file is quarantined and an administrator is notified. PSES also allows users with enterprise roles to monitor user activity (such as who made changes to a record, what was changed, and when) as well as data input. System developers can use the embedded tools to look further into the history and changes made to a record if necessary.

PII in PSES includes information provided by the subject on a DOT form, background investigative request form, or other documents. Authorized users entering PII into PSES are responsible for ensuring the accuracy and completeness of submitted information. Documents are visually inspected against data inputs to ensure transcription accuracy and then as each step in the PerSec process is completed the initial data is validated by adjudicators reviewing the record against the completed investigation which includes copies of the original documents completed by the subject. PSES performs data validation on information stored in the system by comparing information received from internal and external systems. See Appendix B for a list of systems that interface with PSES.

Individuals with records in PSES also can correct information when they receive their PIV card. If the PIV card has inaccurate information, for example, the name is misspelled, records will be researched to identify and correct the discrepancy.

Security

DOT shall implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

PII is protected by reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under the Federal Information System Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems, dated March 2006, and NIST Special Publication (SP) 800-53 Rev.4, Recommended Security Controls for Federal Information Systems and Organizations, dated August 2009. The Department has a comprehensive information security program that contains management, operational, and technical safeguards that are appropriate for the protection of PII. These safeguards are designed to achieve the following objectives:

- Ensure the security, integrity, and confidentiality of PII
- Protect against any reasonably anticipated threats or hazards to the security or integrity of PII
- Protect against unauthorized access to or use of PII

PSES is designed to meet all current cyber security requirements for protecting privacy information while still allowing only authorized users the full transparency needed to complete the personnel security process for applicants, employees and contractors. PSES records are safeguarded in accordance with applicable rules and policies, including all applicable Department automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in PSES 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 and permissions. PSES is protected from unauthorized access through appropriate administrative, physical, and technical safeguards and all system access is logged and monitored.

Logical access to the system is guided by the principles of least privilege and need to know. Role-based user accounts are created with specific job functions allowing only authorized accesses, which are necessary to accomplish assigned tasks in accordance with compelling operational needs and business functions of the system. Any changes to user roles required approval of the System Manager.

The Department maintains an auditing function that tracks all user activities in relation to data including access and modification. Technical security controls include firewalls, intrusion detection, encryption, access control list, and other security methods. Department personnel and contractors supporting the system are required to attend security and privacy awareness training and role-based training offered by the Department. No access will be allowed to PSES prior to receiving the necessary clearances and security and privacy training as required by the Department. All users at the federal level are made aware of the Rules of Behavior (ROB) for IT Systems prior to being assigned a user identifier and password and prior to being allowed access to PSES. The PSES system tracks in an audit file each entry to ensure data integrity and record accuracy.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

OST/M-40/Personnel Security is responsible for identifying, training, and holding Agency personnel accountable for adhering to Department privacy and security policies and regulations. The Department follows the Fair Information Principles as best practices for the protection of information associated with PSES. In addition to these practices, policies and procedures are consistently applied, especially as they relate to protection, retention, and destruction of records. Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, processing, and securing data. Guidance is provided in the form of mandatory annual security and privacy awareness training as well as acceptable Rules of Behavior. The Department Chief Privacy Officer conducts regular periodic security and privacy compliance reviews of PSES consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems.

Responsible Official

Linda Guier
Associate Director,
Office of Personnel Security, HSPD-12 and ID Media

Approval and Signature

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer

Appendix A – PSES Forms

The following forms are issued by the Office of Personnel Management (OPM) and are used by all Federal agencies.

- SF-85, Questionnaire for Non-Sensitive Positions
- SF-85P, Questionnaire for Public Trust Positions
- SF-86, Questionnaire for National Security Position
- OF-306, Declaration of Federal Employment
- SF-312, Classified Information Nondisclosure Agreement
- SF-4414, Sensitive Compartmented Information Nondisclosure Agreement
- DD-254, Contract Classification Specification

The following are internal DOT forms:

- DOT 1681, Form to request ID Cards (incl. HSPD-12 PIV)
- DOT 1600.8, Personnel Security Action Request and Notification
- DOT-1631, Credit Release

Appendix B – Internal and External Department Sharing

In support of the Department's use of PSES to manage its background investigation requirements, data in PSES may be shared with the following internal systems for data integrity matching and reducing manual data input.

Internal Systems

- **Federal Aviation Administration (FAA)/ CASTLE Consolidated Information Repository (CASTLE/IR)** – collects standard interface files plus additional data elements needed to update personnel security interfacing applications. This includes subject PII such as name, date and place of birth, addresses, position designation.
- **FAA/eDelivery -** DCSA only provides a single connection to agencies for its data. Because the FAA is the largest personnel grouping within the DOT, the FAA hosts the connection between the DOT and DCSA. The eDelivery system is used to send FAA a digital file of all the closed cases released by DCSA for a given day. After FAA receives the file, they parcel out their investigations from the eDelivery package and send the remaining cases to PSES through a secure connection. PSES takes the completed investigations and attaches them to the specific subject's record and flags the record for the supervisor of the adjudications group. The supervisor then assigns an adjudicator to review the record for a final determination. This is a receipt only connection where PSES receives the completed investigation for adjudication purposes.
- **FAA/HSPD-12 -** The FAA requires ad hoc access to PIV approval status information to support issuance of PIV cards for DOT employees and contractors. Basic PII is shared and compared for compliance with HSPD-12 issuance policy to ensure a scheduled/completed investigation is on file and the issuance of a PIV card is approved.

External Systems

- **Department of Interior (DOI)/Workforce Transformation Tracking System (WTTS)** – The WTTS system is used to obtain and provide Federal Employee Position Information with the WTTS system in an ad hoc manner. This data is used to ensure there is a record of each new hire or a record of any position change for a current employee to ensure the background investigation matches the position designation per Federal regulations.
- **Department of Justice (DOJ)/Civil Applicant System (CAS)** - System is to obtain the Fingerprint Check results as part of the Federal level checks required for background investigations and PIV card issuance. Facilitates improved data integrity by comparing basic PII between the fingerprints and PSES data.
- **Department of Defense (DoD)/National Background Investigation Systems (NBIS) -** NBIS is used to send DCSA Security Data used conduct the background investigation upon which hiring decisions and the granting of national security clearances are made.
- **Office of the Director of Nation Intelligence (ODNI)** – Office of the Director of National Intelligence requires all Federal Agencies to provide Personnel Security Metrics on all of

DOT's National Security Cleared employees and contractors. A report is run in PSES and the metrics data is compiled into an Excel spreadsheet and sent to ODNI. No PII is included in the data provided to ODNI.