Privacy Impact Assessment
for the

HRAccess Program

July 28, 2009

Contact Point
Mohammed A. Taher, Program Manager
Transportation Security Administration
Office of Human Capital
Mohammed.Taher@dhs.gov

Reviewing Officials
Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration
TSAPrivacy@dhs.gov

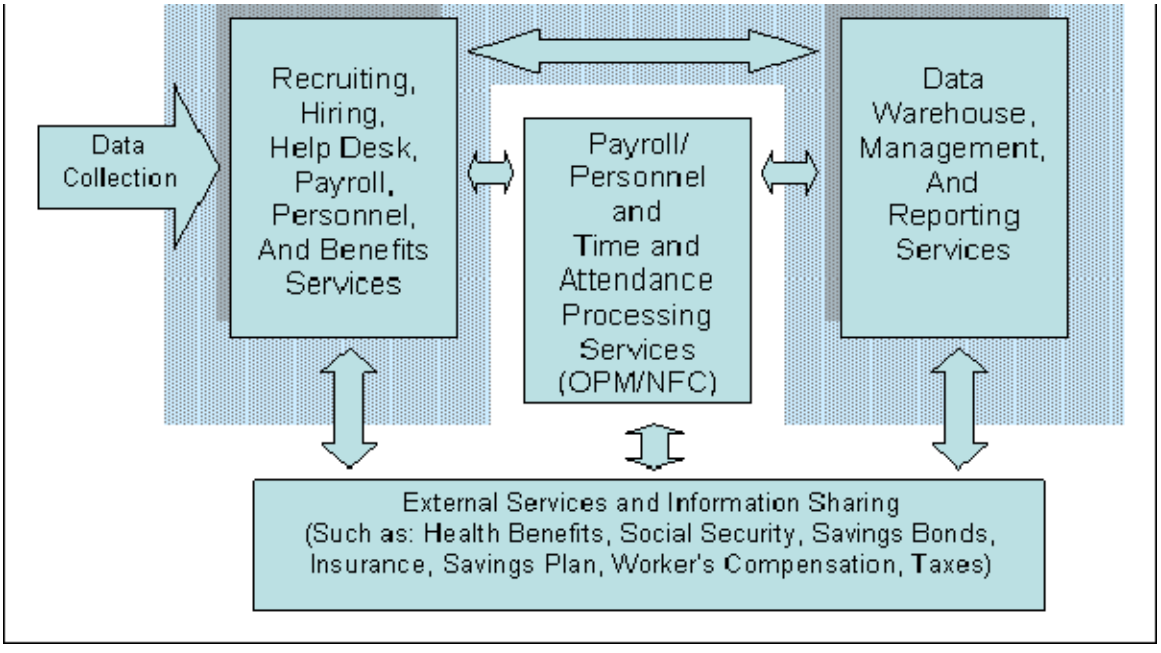
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Privacy@dhs.gov

Abstract

The Department of Homeland Security (DHS) Transportation Security Administration (TSA) is implementing a new program designed to integrate a series of electronic and manual human capital services that were previously managed by separate systems or service providers. Under the HRAccess Program, TSA is streamlining human capital functions utilized to collect, store, and disseminate payroll, benefits, and other workforce-related information for employees and candidates (Unless otherwise noted, hereinafter individual(s) will refer to both an employee and a candidate). This program does not constitute a new collection of information. However, TSA is issuing this Privacy Impact Assessment because this program entails a new system for collecting information about members of the public in an identifiable form.

Overview

The TSA workforce population is located in more than 450 airports in all 50 states, the District of Columbia and U.S. territories. The TSA Office of Human Capital (OHC) initiated the HRAccess Program to combine the services currently being furnished by three contracts into a single contract to streamline and integrate the delivery of services for all employees and candidates. This will enable TSA to manage a single service vendor in human capital services. As part of these changes, TSA has transformed the Entry-on-Duty (EOD) process from paper-based to electronic. EOD forms are standard government forms or TSA-specific forms. The below graphic depicts the various services provided by the HRAccess service provider.



Recruiting, Hiring, Help Desk, Payroll, Personnel, and Benefits Services:

- TSA hires a large number of personnel each year in order to meet the human capital needs of the agency. TSA collects Personally Identifiable Information (PII) about candidates in order to properly review, assess, and determine if the candidate has the knowledge, skills, and abilities for the position under consideration. The HRAccess Program will provide for a consolidated recruitment and hiring system which will be electronically linked to the TSA personnel system. It also links to the OPM USAJOBs system.

- When TSA hires a new employee, TSA collects PII from and about the employee and enters the information into the TSA personnel system and into the time and attendance system in order to establish the new employee's accounts. From there the information may flow into other internal systems used to administer and manage the human capital operations of the agency, including payroll and benefits.

- TSA enters additional data in the personnel and associated systems whenever an employee's status changes due to hiring actions, promotions, pay increases, transfers, awards, change of benefits, etc. The HRAccess program will provide a rapid and sure way to collect the information and process it. This information is sent to the U.S. Department of Agriculture's (USDA) National Finance Center (NFC) daily to be entered into their Payroll/Personnel system.

- TSA provides Help Desk services to TSA employees who have personnel related problems or questions.

Payroll/Personnel and Time and Attendance Processing Services (OPM/NFC)

- NFC supplies the payroll and personnel action processing services and time and attendance services for TSA under the direction of DHS.

- NFC processes the payroll for TSA based on personnel and payroll action updates received from TSA. To process the payroll properly, NFC requires up-to-date position, personnel, benefits, and time and attendance data about the individual. Position, personnel, and benefits changes are provided to NFC whenever the changes are approved. Time and attendance data is collected for each pay period and used to calculate pay. This net pay amount is sent to the U.S. Treasury, which transmits the amount electronically to the employee's bank account or mails a paper check to their residence address. NFC also prepares the Leave and Earnings statement for each employee and posts it on the employee self-service web site, where it can be read and printed by the employee.

- NFC assists TSA in managing benefits by withholding the proper amount of money from each paycheck for benefits the employee has elected to receive. TSA transmits these amounts along with a notation of the affected employee to the respective benefits providers.

- NFC also sends information from each employee's records to the U.S. Office of Personnel Management (OPM) for use in managing the workforce.

Data Warehouse, Management, and Reporting Services:

- TSA uses the Data Warehouse system to collect data from the NFC after it has been processed. This data is used to manage the human capital of TSA and to monitor the effectiveness of personnel and payroll information processing.

External Services and Information Sharing:

- Human capital data is shared externally in accordance with the Privacy Act to include such activities as providing information to a court in deciding child support, alimony, or garnishment issues and to support the benefits elected by employees such as with the Bureau of Public Debt for saving bonds, the Federal Retirement Thrift Investment Board for thrift savings plans, and with various authorized benefits providers, or for other authorized allotments such as Combined Federal Campaign.

Section 1.0 Characterization of the Information

1.1 What information is collected, used, disseminated, or maintained in the system?

TSA will collect information such as that listed below from TSA employees and candidates in order to complete official personnel actions, basic benefits, pay, cash awards, and leave records of TSA employees and candidates and in order to conduct the background investigations or other national security investigations.

- Full Name
- Other Names Used
- Social Security Number (SSN)
- Driver's license number
- Passport number
- Date of Birth
- Alien registration number/Form I-9
- Gender
- Copies of identity source documents
- Eye Color
- Weight
- Height
- Hair Color
- Home Address
- Home Phone Number
- Mobile Phone Number
- Citizenship
- Photograph
- Medical Information
- Testing results
- Financial Information (account numbers or Electronic Funds Transfer Information)
- Account Passwords or personal identification numbers (PINs)
- Fingertip image
- Dependent information
- Beneficiary Information and designations
- Resumes or other qualification documentation

TSA will also collect, use, disseminate, or maintain human capital-related data and/or program information for the purpose of conducting official personnel transactions or to administer programs. Such information includes:

- Work Address
- Employing Organization
- Salary
- Pay plan
- Hours Worked
- Overtime
- Compensatory time
- Leave accrual rate
- Leave usage and balances
- Civil Service Retirement and Retirement System contributions
- FICA withholdings
- Federal, state, or city tax withholdings
- Federal Employee Health Benefits withholdings
- Garnishments
- Savings Bond allotments
- Union dues withholdings
- Deductions for IRS levies
- Thrift Savings Plan contributions
- Court ordered child support levies
- Court ordered alimony
- Employee Relations Records
- Federal salary offset deductions
- Leave Transfer Program Information
- Leave Bank Program Information
- Educational level
- Specialized education or training obtained outside the Federal Government
- Beneficiary Designations
- Work experience
- Personal References
- Race, nationality, origin

1.2 What are the sources of the information in the system?

The HRAccess Program will typically collect PII directly from the individual or their representative. Other sources of information may include such third-party sources as a court, references, healthcare provider and/or health service organization, in appropriate circumstances.

1.3 Why is the information being collected, used, disseminated, or maintained?

The information is being collected, used, disseminated, or maintained in order to facilitate and manage personnel transactions and human capital functions for candidates and employees.

1.4 How is the information collected?

Information concerning candidates and employees in the system is collected from the individual in person, by telephone, in paper form, via electronic forms, by email, or from facsimile. Information is also collected from electronic input devices such as time clocks, login devices, or security screening

devices, which record the individual's entry or departure from work assignments or work areas. TSA may also receive information from courts, healthcare providers, health service organizations or tax authorities in paper format.

1.5 How will the information be checked for accuracy?

TSA will collect PII directly from the individual or his or her representative submitting the form, request, or applying for an agency benefit or program. Because the individual provides the majority of information about him or herself directly, the likelihood of erroneous PII is minimized. In some instances, TSA must rely on third-party information that may be subjective, such as personal references for which accuracy may not be established.

Data is also checked for accuracy by Human Resource Specialists, Administrative Officers, supervisors, managers, other officials, and contractors authorized to review data. These individuals will notify the affected individual when there appears to be an inaccuracy and request that the individual correct the data before it is entered into the system.

Employees can check their personnel and payroll data by viewing the Statement of Earnings and Leave (SEL), W-2 Forms, or information screens available through the employee self service system provided by the Agency.

Employees may use the web-based OPM Electronic Official Personnel Folder (eOPF) system to view and check official documents, Notification of Personnel Action forms and associated supporting documents. For security purposes, an individual PIN number may be required to view this information.

Information received from a court or tax authority is assumed to be accurate.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

TSA's general operating authorities are set forth in the Aviation and Transportation Security Act (ATSA) 49 U.S.C. § 114(f). Authority for collecting general personnel record, employee performance files, and medical file data are defined in 5 U.S.C. § 301, 1104, 1302, 1303, 2302(b)(10), 2951, 3301, 3321, 3372, 4118, 4305, 5112, 5405, 8347, and Executive Orders 9397, 9830, 10450, and 12107.

DHS has established Service Level Agreements (SLAs) with the USDA NFC that provide authority for departmental components, including TSA, to utilize both human capital and payroll/personnel information technology systems to perform agency administration functions.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The privacy risk associated with the collection of this information for the purpose of managing human capital-related transactions is that it may be mishandled or exposed to unauthorized persons. HRAccess automates many document submission processes by using secure information technology

procedures that will minimize the opportunity to mishandle this information. Unauthorized release of personally identifiable information is mitigated through the use of multiple levels of security and through personnel training and monitoring. Those individuals who handle personal information are required to undergo periodic training in handling individual data and sensitive security information. Data is maintained within facilities that have limited access. Electronic data is maintained in databases with role-based security to limit access to personnel who have a need to know the information in the performance of official duties. Misidentification is an additional privacy risk. TSA seeks to reduce the potential for misidentification by requesting sufficient items of information in order to distinguish the individual from others that may have the same name.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

TSA will use information gathered from individuals to make qualification and hiring decisions, administer and manage pay, benefits, employee performance, maintain health related information about the individual, and other human resource-related information and transactions and to comply with court orders. The information is also used to establish a source of official data concerning employment with the Agency. TSA will use the information to monitor statistical data to assess the agency's progress in meeting equality and equal opportunity in employment, promotion, and other goals.

E-Verify will be used to check the work status of new hires online by comparing information from an employee's I-9 form against Social Security Administration and DHS Databases.

Information received from the TSA Personnel Security Division as a result of a required security investigation or background investigation may be used to disqualify a candidate or employee from government service.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Data provided by employees and candidates, may be used to generate statistical and forecasting information used for DHS and TSA management decisions. DHS and TSA may use statistical analysis computer programs, online analytical processing computer programs, or other suitable programs and techniques to collect, categorize, analyze, and display the data. TSA may use the data to help TSA identify issues in need of improvement within its human capital procedures as described above.

Additionally, information may be provided to OPM and other authorized agencies for the purpose of performing statistical analysis of employment patterns. Information may be provided for computer matching purposes using comparison tools to identify individuals who are indebted to the government or for other authorized purposes.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

HRAccess does not use commercial data, but may use publicly available data for certain positions where publicly available information may have a bearing on suitability. For example, if a news story report that an employee had been arrested for theft, that information as well as arrest records or other public records might be included in the Employee Relations files as part of what generated discipline or adverse action. By way of further example, if an employee posts inappropriate images on a web-site affecting the reputation of the agency (such as in uniform), those images might be retained as part of the disciplinary file.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The privacy risks associated with this collection include the unauthorized or inadvertent release of PII collected over the normal workflow process of managing personnel and their case files. Unauthorized browsing for information on specific or groups of information for non-official purposes is an additional risk. To mitigate these risks, TSA has implemented mandatory personnel security policies and procedures that require all personnel to be the subject of a favorable background investigation prior to being granted access to sensitive information systems. TSA also requires completion of appropriate access agreements (e.g., nondisclosure, acceptable use, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access. In addition, TSA also requires all personnel to complete privacy awareness training. Auditing functions permit the reconstruction of security relevant events. Another risk is that publicly available data is inaccurate. Depending on the data, TSA mitigates this risk by permitting employees to contest the basis of disciplinary action.

Section 3.0 Retention

3.1 What information is retained?

TSA HRAccess retains records associated with hiring and employment of its work force, including such records as:

- Official Personnel Folders (OPFs)
- Personnel Correspondence Files
- Offers of Employment Files
- Recruiting, Examining, and Placement Records
- Certificate of Eligibles Files
- Position Classification Files and Position Descriptions
- Survey Files
- Classification Appeals Files
- Interview Records
- Performance Rating Board Case Files
- Temporary Individual Employee Records
- Employee Awards Files

- Incentive Awards Program Reports
- Notifications of Personnel Actions
- Personnel Operations Statistical Reports
- Correspondence and Forms Files
- Supervisors' Personnel Files and Duplicate OPF Documentation
- Individual Non-Occupational Health Record Files
- Health Unit Control Files
- Employee Medical Folder (EMF)
- Employee Health Statistical Summaries
- Employee Performance File System Records
- Reasonable Accommodation Request Records
- Equal Employment Opportunity (EEO) Records
- Personnel Counseling Records
- Alternative Dispute Resolution (ADR) Files
- Labor Management Relations Records
- Training Records
- Personal Injury Files
- Merit Promotion Case Files
- Examining and Certification Records
- Occupational Injury and Illness Files
- Denied Health Benefits Requests Under Spouse Equity
- Federal Workplace Drug Testing Program Files
- Donated Leave Program Case Files
- Wage Survey Files
- Retirement Assistance Files
- Handicapped Individuals Appointment Case Files
- Pay Comparability Records
- Alternate Worksite Records
- Electronic Mail and Word Processing System Copies
- Individual Employee Pay Record
- Noncurrent Payroll Files
- Leave Application Files
- Time and Attendance Source Records
- Time and Attendance Input Records
- Leave Records
- Tax Files
- Savings Bond Purchase Files
- Combined Federal Campaign and Other Allotment Authorizations
- Thrift Savings Plan Election Form
- Direct Deposit Sign-up Form (SF 1199A)
- Levy and Garnishment Files
- Payroll Change Files
- Retirement Files
- Payroll System Reports
- Payroll Correspondence

3.2 How long is information retained?

TSA HRAccess program records will be retained and disposed in accordance with applicable Government-wide National Archives and Records Administration's (NARA) General Records Schedules. These schedules have varying retention requirements depending on the category of records maintained. The specific records retention periods for the items in Section 3.1 above can be obtained by reviewing NARA’s listing of General Record Schedules.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes. NARA has approved government-wide record retention schedules for human capital-related records. HRAccess Records are retained in accordance with the provisions of NARA's General Records Schedules 1 and 2.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The privacy risks associated with data retention is data security. This risk is mitigated by continually monitoring and auditing the systems where the data is maintained in accordance with the requirements of Federal Information Security Management Act (FISMA). Additionally, security procedures and controls are continuously updated as new information, processes, and technology become available to counter threats. Information collected in connection with this program will be maintained in accordance with NARA-approved record retention schedules.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

The HRAccess Program provides human resources services for the agency. Information will be shared within DHS with those personnel who have a need for the information in the performance of their duties. For example, the Office of Human Capital will share information within DHS to manage and administer job classifications, payroll actions, timekeeping information and systems, benefits, performance evaluations, and leave transactions. Information is expected to typically be shared with offices such as Ombudsman, Civil Right and Liberties, Chief Counsel, Legislative Affairs, Inspection, Privacy, Freedom of Information, and other offices on employment matters or to respond to inquiries. The TSA Office of Human Capital also shares information with the TSA Personnel Security Division (PSD) in order to identify an employee or candidate for a required background or security investigation.

4.2 How is the information transmitted or disclosed?

TSA will transmit HRAccess information within DHS in person, in paper format, via a secure or encrypted data network, on a password-protected CD, via facsimile, or telephonically to those who have a need for the information in the performance of their official duties. The method of transmission may vary according to specific circumstances.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Given the enterprise nature of the HRAccess Program, the privacy risk associated with sharing this information is the possibility the data may be transmitted or disclosed to individuals who do not have a need to know the information. This risk is mitigated by administrative controls including training of personnel, and technological controls on system data such as security credentials, passwords, real-time auditing that tracks access to electronic information.

Section 5.0 External Sharing and Disclosure

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

TSA will share information with the NFC, OPM, and other federal, state, local, or tribal organizations to perform payroll, benefits, and other workforce-related transactions or services in accordance with the Privacy Act and applicable system of records notices. TSA will also share human capital-related information with external organizations pursuant to the Privacy Act and the routine uses identified in applicable government-wide Privacy Act system of records notices (SORNs).

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Yes. The information is shared in accordance with the following Privacy Act SORNs

SORN Number and Title	Last Publication Date	Federal Register Citation
DHS/TSA-022, National Finance Center Payroll/Personnel System (NFC)	July 17, 2006	71 FR 40530-40532
OPM/GOVT-1 General Personnel Records	June 19, 2006	71 FR 35342-35347
OPM/GOVT-2 Employee Performance File System Records	June 19, 2006	71 FR 35347-35350
OPM/GOVT-3 Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers	June 19, 2006	71 FR 35350-35351

OPM/GOVT-5 Recruiting, Examining, and Placement Records	June 19, 2006	71 FR 35351-35354
OPM/GOVT-6 Personnel Research and Test Validation Records	June 19, 2006	71 FR 35354-35356
OPM/GOVT-7 Applicant Race, Sex, National Origin, and Disability Records	June 19, 2006	71 FR 35356-35358
OPM/GOVT-9 Position Classification Appeals, Job Grading Appeals, and Retained Grade or Pay Appeals	June 19, 2006	71 FR 35358-35360
OPM/GOVT-10 Employee Medical File System Records	June 19, 2006	71 FR 35360-35363
DOL/GOVT-1, Federal Employees' Compensation Act File	April 8, 2002	67 FR 16826-16829
MSPB/GOVT-1 Appeals and Case Records	November 21, 2002	67 FR 70254-70256
OGE/GOVT-1 Executive Branch Public Financial Disclosure Reports and Other Ethics Program Records	January 22, 2003	68 FR 3099-3101
OGE/GOVT-2, Confidential Statements of Employment and Financial Interests	January 22, 2003	68 FR 3101-3103
TREASURY/BPD.002, United States Savings-Type Securities – Treasury/BPD	July 23, 2008	72 FR 42906-42909
Social Security Administration 60-0059	January 11, 2006	71 FR 1819-1823

The information shared with NFC is also governed by SLAs between the NFC and DHS that provide authority for departmental components, including TSA, to utilize both human capital and payroll/personnel information technology systems to perform agency administration functions.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Depending on the recipient and the urgency of the request or disclosure, the information may be disclosed in person, telephonically, electronically via a secure data network, via facsimile, or via password protected CD.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

The privacy risk associated with sharing this information with external stakeholders is the opportunity for dissemination to individuals who do not have a need to know the information in the performance of their official duties. TSA will limit sharing of this information under the applicable provisions of the SORN and the Privacy Act. By limiting the amount of information collected, and sharing of this information to those who have an official need to know, TSA is mitigating attendant privacy risks.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information?

Yes. Forms that collect personal information contain a Privacy Act Statement. The publication of this PIA and the Privacy Act SORNs listed in Section 5.2 above also serve to provide public notice of the collection, use and maintenance of this information.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Individuals have the opportunity to decline to provide information requested. However, failure to provide certain items of information or comply with required drug testing may affect benefits, rights, and employment. In addition failure to provide requested information may delay the process of delivering benefits and personnel actions to the individual, because it might increase the time necessary to identify the individual and verify that the individual is authorized the benefits.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Individuals do not have the right to limit the uses of information provided as part of their employment or application for employment. Individuals may opt not to provide information.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

In addition to the Privacy Act SORNs, individuals are provided a Privacy Act Statement on the associated forms or online applications prior to providing the information and may therefore determine if he or she would like to submit the information. Additionally, candidates are on notice that third parties may be consulted regarding employment qualifications candidates have provided.

Section 7.0 Access, Redress and Correction

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

Once hired, current employees may be granted user IDs and passwords that will allow them to gain access to and amend their own personal information contained in designated human capital information systems.

Individuals may also submit a Freedom of Information Act/Privacy Act (FOIA/PA) request to TSA in writing by mail to the following address:

Transportation Security Administration, TSA-20

FOIA Division

601 South 12th Street

Arlington, VA 20598-6020

FOIA/PA requests may also be submitted by fax at 571-227-1406 or by filling out the Customer Service Form (URL: http://www.tsa.gov/public/contactus). The FOIA/PA request must contain the following information: Full Name, address and telephone number, and email address (optional). Please refer to the TSA FOIA web site (http://www.tsa.gov/public).

7.2 What are the procedures for correcting inaccurate or erroneous information?

Individuals may correct inaccurate or erroneous information in the system that pertains to them by writing to the TSA Office of Human Capital at the following address:

Transportation Security Administration, TSA-21

Director, Human Resources Information Systems

601 South 12th Street

Arlington, VA 20598-6021

Individuals seeking to correct information in their records should provide their full name and a description of information that they seek to correct and the reason why the information is incorrect.

7.3 How are individuals notified of the procedures for correcting their information?

The publication of this PIA and of the applicable SORNs serves to provide public notice of the collection, use, and maintenance, and means of correcting this information.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Appropriate redress is provided.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Individuals may correct their information at any time during which TSA possesses and uses their information. Any risks associated with correction of information are thoroughly mitigated by the individual's ability to correct their information. Further, individuals may request access to or correction of their personal information pursuant to the procedures outlined in this PIA and in accordance with DHS procedures for requesting amendment of records at 6 C.F.R. § 5.26.

Section 8.0 Technical Access and Security

8.1 What procedures are in place to determine which users may access the system and are they documented?

Role-based access controls are employed to limit the access of information by different users and administrators based on a need to know. TSA also employs processes to enforce separation of duties to prevent unauthorized disclosure or modification of information. No unauthorized users are permitted access to system resources. Adherence to access control policies is enforced in coordination with and through oversight by TSA IT Security Officers.

8.2 Will Department contractors have access to the system?

Yes. TSA will hire contractors to perform human capital services and to perform routine IT maintenance, record processing, and security monitoring tasks in order to perform their official duties. TSA Contractors are under obligation to follow the privacy and security requirements of the Department. All contractors having access to DHS systems are required to undergo a background investigation and to sign Non-Disclosure Agreements.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All TSA and assigned contractor staff receive TSA-mandated privacy training on the use and disclosure of personal data. Compliance with this training requirement is audited monthly by the TSA Privacy Officer, and failure to complete the training is reported to program management for remedial action. CD-ROM-based training modules are provided to TSA Contractors not assigned to TSA facilities or those that do not have access to TSA Network Resources.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Certification and Accreditation was completed on December 30, 2008. The system will be reviewed whenever major changes are implemented and the certification documentation will be updated to reflect current security controls in alignment with federal information processing standards.

Information in this system will be safeguarded in accordance with FISMA. The system will operate under the legal authority of the Designated Accrediting Authority (DAA) who manages personnel, operations, maintenance, and budgets for the system and field components.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

TSA has implemented security controls and technology features that incorporate protection of privacy. TSA has complied with FISMA and NIST protocols and procedures, and mitigated privacy risks through the following methods:

- Role-based user accounts control access to the system.
- User accounts are audited to monitor system access and FISMA compliance.
- The system controls the transmission and storage of data.
- All government and contract personnel are required to complete privacy and information security training.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Data on the system is secured in accordance with applicable Federal standards. Security controls are in place to protect the confidentiality, availability, and integrity of personal data, including role-based access controls that enforce a strict need to know policy. Physical access to the system is strictly controlled with the use of proximity badges. The systems are housed in controlled environments within secure facilities. In addition, administrative controls, such as periodic monitoring of logs and accounts, help to prevent and/or discover unauthorized access. Audit trails are maintained and monitored to track user access and unauthorized access attempts.

Section 9.0 Technology

9.1 What type of project is the program or system?

The HRAccess Program is a collaboration of commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS) information technology systems used to provide human capital services through a

contractor that provides enterprise-wide support. The contractor also develops integrated systems to support the required services. System components include COTS/GOTS hardware and operating systems.

9.2 What stage of development is the system in and what project development lifecycle was used?

The system is being developed under the System Development Life Cycle (SDLC) process developed by TSA. The system is currently in the development stage of the SDLC. Between contract award and full operational capability, the system will progress through the following phases of the SDLC: Design, Development, Testing, and Implementation. Once the Deployment Approval decision has been attained, the system will enter the Operations and Maintenance stage of the SDLC.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

TSA is developing a time and attendance system that is expected to utilize a fingertip image and a PIN to record workplace arrival and departure information. This two-factor authentication process contributes to mitigate risks of misidentification, promote accuracy, and reduce handling of time and attendance information.

This tool replaces the traditional time clocks located at many work locations. The device does not retain the fingertip image. Instead, particular data about the fingertip captured during the enrollment process is stored in a smaller encrypted template on a secured TSA network. The device transmits an encrypted mathematical representation of the fingertip to TSA in order to match the image to the template stored on the secured network. To further mitigate privacy concerns, the transmission from the device at the work location to TSA is encrypted as well.

Approval Signature Page

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security