# Privacy Impact Assessment
## For the

# Personnel Security Activities Management System

**September 12, 2007**


**Contact Point**
**John Pardun, System Owner**
**Deputy Chief, Training & Operations Security**
**Department of Homeland Security**
**(202) 447-5415**

**Kevin Crouch**
**Division Chief, Training & Operations Security**
**Department of Homeland Security**
**(202) 447-5424**

**Reviewing Official**
**Hugo Teufel III**
**Chief Privacy Officer**
**Department of Homeland Security**
**(703) 235-0780**

## Abstract

The Department of Homeland Security Office of Security uses the Personnel Security Activities Management System (PSAMS) to automate the tracking of the status of Personnel Security related activities at DHS headquarters.

## Introduction

The Personnel Security Activities Management System (PSAMS) automates the tracking of the Personnel Security related activities at the Department of Homeland Security (DHS) headquarters. The purpose of PSAMS is to support the activities of the DHS Office of Security and related Administrative Center Security Offices with electronic storage of status and completion dates of various security checks and an integrated process and workflow management system.

PSAMS serves as a mechanism to track status of security checks related to the processing of an individual's security clearance. PSAMS provides for the electronic storage of security process tracking information, enhancing the ability of authorized personnel to retrieve information, and allowing reduction in the volume of paper documents. The system also automates exports and imports of information necessary for information exchange with other government agencies in order to reduce error rates and potential delays in processing security documents.

This system contains Security Clearance Management information for DHS personnel, contractors, consultants, student interns, visitors, and others who have access to DHS facilities. The detailed information collected as part of the clearance process and its results (such as background investigations) are not kept in PSAMS, but rather in separate hard copy files that are maintained in a controlled access file room.

The records in this system reflect the tracking/status of security clearances checks and associated activities needed for the management and implementation of Office of Security programs and activities that support the protection of the Department's personnel, property, facilities, and information. These records include, but are not limited to the current status of, investigation and adjudication of personnel security and suitability determinations; investigation and suitability determinations for access to classified national security information and sensitive but unclassified information; and verification of eligibility for access to classified national security information.

This PIA provides detail about the use of Office of Security records maintained within the PSAMS system which covers not only DHS employees, but also contractors, consultants, student interns, visitors, and others who have access to DHS facilities. The personally identifiable information contained in this system consists of data elements necessary to identify the individual and to perform and track background or other investigations and other security related processes concerning the individual. This system has been designed to closely align with the Office of Security's business practices.

PSAMS data is primarily used internally by DHS with the following exceptions: background investigation process, clearance verification, and employment eligibility information and relevant personally identifiable information, which are shared with the Office of Personnel Management, the Scattered Castles Secure Compartmented Information (SCI) database, and the Personal Identity Verification (PIV) Management System for the Homeland Security Presidential Directive 12 (HSPD-12) system.

# Section 1.0 Information Collected and Maintained

## 1.1 What information is to be collected?

The personally identifiable information collected consists of data elements necessary to identify the individual and to track completion of security related processes including background or other investigations concerning the individual. The system has been designed to closely align with the Office of Security's business practices.

PSAMS collects and maintains the following personal identifiable information:

- Full Name
- SSN
- Address
- Date of Birth
- Place of Birth
- Gender
- Eye Color
- Hair Color
- Height
- Weight
- Race
- Duty Location

PSAMS collects and maintains the following clearance verification information:

- Employee Type
- Organization
- Position Title
- Position Sensitivity
- Access Level
- Whether clearance forms have been received & date received
- Date clearance forms validated as complete & correct
- Whether fingerprints have been forwarded to FBI
- Date Fingerprint results received from FBI
- Credit Check completed & date completed
- NCIC Check completed & date completed
- FBI Name Check via Tape – request & result received dates
- Security Investigation types & date(s) completed
- Approval to Enter-on-Date
- OPM investigation scope
- SCI Clearance certification dates including brief & debrief dates
- Security Training dates
- Suitability determination, for example the date and the fact that the security checks have been completed

The background information collected as part of this process and its results are kept in separate background investigation files, but the completion of the investigations are tracked in the PSAMS system. NCIC Check, Credit Check and FBI Name Check completion dates are stored within PSAMS; however, check results are not stored within the system. OPM clearance information and National Finance Center updates may also be included.

## 1.2 From whom is information collected?

Information is collected directly from DHS employees, contractors, consultants, student interns, visitors, and others who require access to DHS facilities and systems. The information is

also collected from the individuals conducting the background investigation in order to update the system relating to the status of particular activities.

## 1.3 Why is the information being collected?

The information identified above is used to track to completion security vetting requirements. The suitability review and determination is a requirement to work at DHS. Personnel Security staff record suitability review and determination information to reduce risk of allowing access to DHS information and facilities by personnel with a criminal record or possible ties to terrorism. If persons decline to provide necessary information to complete this information, they cannot be hired as a permanent employee, or work at the agency as a contractor long-term (over 6 months).

## 1.4 How is the information collected?

Information for PSAMS is entered by employee candidates and contractors via the SF85 and SF86 forms. The data is collected either electronically via the OPM eQIP system, or manually entered by DHS Personnel Security Division (PSD) staff from information provided by applicants. The preferred method is electronic transfer of the information entered in the eQIP system based on employee entry. The eQIP system was created by order of the Office of Management & Budget (OMB) as part of the eGovernment initiative and is administered by OPM. It serves as a central location for the collection of applicants data necessary to support security clearance investigations. Information, including submission of needed forms and completion of required investigations are updated by DHS Personnel Security Division.

## 1.5 What legal authorities defined the collection of information?

Depending on the type of investigation required, Executive Orders 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; and parts 5, 731, 732, and 736 of Title 5, Code of Federal Regulations provide the basis for collecting information regarding background investigations for National Security Positions.

Protection of information associated with the system is described in DHS Management Directive (MD) 11042.1 Safeguarding Sensitive and Unclassified Information (FOUO), and DHS Policy for FOIA Compliance MD 0460.1

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

In order to minimize the amount of personally identifiable information in PSAMS, the Office of Security designed the systems so that any investigative information would not be placed in the system.

# Section 2.0 Uses of the System and the Information

## 2.1 Describe all the uses of information.

The records in this system will be used for tracking of all clearance-related processes for the individual during their tenure with DHS. Two paper-based forms are used to initiate the background investigation, Questionnaire for Non-Sensitive Positions Standard Form 85 (SF-85) or the Questionnaire for National Security Positions Standard Form 86 (SF-86). The information from these forms is captured using eQIP and is used as the basis for the security investigation.

The information stored in PSAMS is used to track clearance status information. It is tracked by personal identity, personnel type, and organization. The information is used by DHS Office of Security personnel to track the following:

- Access Level
- Whether clearance forms have been received & date received
- Date clearance forms were validated as complete & correct
- Whether fingerprints have been forwarded to FBI
- Date Fingerprint results were received from FBI
- Credit Check completed & date completed
- NCIC Check completed & date completed
- FBI Name Check via Tape – request & result received dates
- Security Investigation types completed & date(s) completed
- Approval to Enter-on-Date
- OPM investigation scope & source data
- SCI Clearance certification dates including brief & debrief dates
- Security Training dates
- Suitability determination

## 2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

No. This system is used to track security related information and related processes. There are no in-built data analysis functions to identify patterns or new areas of concern.

## 2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

As part of the application process, the individual is required to enter their PII and background information into the Office of Personnel Management e-QIP system. The Office of

Security Personnel Security Division receives the information about the individual from applications provided in the security clearance vetting or suitability review process. PII for Federal employees is verified by a comparison with data provided by the National Finance Center (NFC). That information is vetted thru FBI fingerprint check, Credit check, NCIC check, FBI name check, OPM background investigation and other investigation(s) as deemed necessary based on DHS Suitability or National Security requirements.

### 2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

Personally identifiable information that is needed is provided by the individual through a secure portal known as eQIP maintained by OPM in order to obtain needed information to conduct the necessary background checks. The basic personal identifiable information as outlined in Section 1.1.above, is used to create a record in PSAMS for ongoing security related process and determination tracking. In order to minimize misuse of the information access controls, training, and audit mechanisms have been put in place to ensure appropriate use of the information within the system.

In order to mitigate the risk of PSAMS and its information being misused the Office of Security has put in place both technical safeguards and training. Access to the PSAMS system requires access to the DHS Internal network. PSAMS user accounts are individually approved by DHS Office of Security Division Chiefs before software required for access is installed. All users have received DHS Computer Security training and have been vetted and cleared for access to PII, sensitive, and classified information. Access to PSAMS is role-based and data access for users of the system is limited to the minimum access needed to perform their respective functions. The capability to update information is restricted to those roles that specifically require this to perform their duties and record changes are tracked and audited through the use of transaction history tracking which provides information on data changes made and the specific user who made the change.

## Section 3.0 Retention

### 3.1 What is the retention period for the data in the system?

DHS Personnel Security Records relating to individuals are retained and disposed of in accordance with General Records Schedule 18, item 22a and 22c, approved by NARA. Records are destroyed upon notification of death or not later than five years after separation or transfer of employee, whichever is applicable. Index to personnel security case files are destroyed with the related case.

### 3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

DHS personnel security files are destroyed in accordance with legal requirements and the disposition instructions in the General Records Schedule 18 issued by the National Archives and Records Administration (NARA).

### 3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

PSAMS maintains the fact that an individual maintains an Sensitive Compartmented Information (SCI) records clearance for two (2) years based on Intelligence Community requirements. Records as maintained as described in Executive Order 12958 – Classified National Security Information, as amended.

Additionally, an individual's data is retained in PSAMS for the full term of their active employment with the Department of Homeland Security. This is in support of related personnel processes and in support of DHS Office of Security mission.

## Section 4.0 Internal Sharing and Disclosure

### 4.1 With which internal organizations is the information shared?

The information is shared with the appropriate Department employees and contractors that require access to security eligibility and access related information to facilitate the investigation and adjudication of personnel suitability and clearances. This includes Personnel Security Division (PSD), Special Security Programs Division (SSPD), and Human Capital. These individuals, by law and contract, are bound by the Privacy Act. Specific information about an individual will be shared with Department employees and its contractors who have a "need to know" regarding the vetting process. Department contractors are contractually obligated to comply with the Privacy Act in the handling, use and dissemination of all personal information.

### 4.2 For each organization, what information is shared and for what purpose?

Both PSD and SSPD, as organizations, have access to the full set of personally identifiable information stored in PSAMS; however, individual employee access is role-based.

PSD uses PSAMS data as a means to make hiring decisions and to process and adjudicate security clearances. SSPD uses PSAMS as a means to process and grant requests for Sensitive Compartmented Information (SCI).

### 4.3 How is the information transmitted or disclosed?

Access to the information is via an authenticated web interface or software client. Access control is role-based and data is only accessible if a specific user has been approved for access to the

data. Information presented on screens is defined based on specific roles and information required to facilitate those functions.

### 4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

This information is shared with other parts of DHS based facility's Security Clearance and Suitability screening processes and is shared internally on a need-to-know basis. The following are in place to mitigate the risk:

- Access to PSAMS requires a DHS domain account and requires that the user be logged into a DHS Intranet accessible computer;
- PSAMS user accounts are individually approved by DHS Office of Security Division Chiefs before they are provisioned;
- All users have received DHS Computer Security training and have been vetted and cleared for access to privacy, sensitive, and classified information;
- Access to PSAMS is role-based: users of the system have access to a limited subset of data based on the concept of least privilege/limited access;
- Write capability is limited to a few roles, is tracked and audited;
- PSAMS has undergone review and met the Certification and Accreditation (C&A) criteria required of a system hosting privacy data.
- A comprehensive set of Management, Operational, and Technical controls are documented in the System Security Plan and have been tested in conjunction with the FISMA Certification and Accreditation process.

## Section 5.0 External Sharing and Disclosure

### 5.1 With which external organizations is the information shared?

This information is shared as necessary to facilitate National Security Clearance reciprocity and access to controlled facilities. Clearance information is shared with the Office of Personnel Management (OPM), the Intelligence Community and with the HSPD-12 Identity Management system in order to facilitate issuance of Personal Identify Verification (PIV) cards in support of HSPD-12.

Background investigation process, and clearance verification and eligibility information as well as relevant personal data will be:

1. Shared with the Office of Personnel Management (OPM) Clearance Verification System.
2. Shared with the Intelligence Community Secure Compartmented Information (SCI) database when needed/appropriate. SCI clearance status information

including clearance eligibility dates, personnel type, organization, clearance level and SCI certification dates is shared.

3. Shared with the Personal Identity Verification (PIV) Management System, the Identity Management System (IDMS) for the Homeland Security Presidential Directive 12 (HSPD-12) system.

4. Shared with other authorized organizations which require access to clearance information, in conformance with the System of Records Notice, Personal Identity Verification Management System (PIVMS), DHS-OS-002, published on September 12, 2006, 71 FR 53697.

This information is shared as necessary to facilitate National Security Clearance reciprocity, access to controlled facilities, and issuance of Personal Identify Verification (PIV) cards in support of HSPD-12.

Information about individuals that is stored for purposes of granting clearances may be given without individual's consent as permitted by the Privacy Act of 1974 (5 U.S.C. § 552a(b)), including to an appropriate government law enforcement entity if records show a violation or potential violation of law.

Information may also be shared with federal, state, or local law enforcement or intelligence agencies or other organizations in accordance with the Privacy Act and the routine uses identified in the Personal Identity Verification Management System (DHS-OS-002).

## 5.2 What information is shared and for what purpose?

PSAMS shares the following personally identifiable information to facilitate National Security Clearance reciprocity, access to controlled facilities, and issuance of Personal Identify Verification (PIV) cards in support of HSPD-12:

- Full Name
- SSN
- Date of Birth
- Security Clearance level
- Clearance eligibility dates
- Other information as defined by OPM to facilitate Security Clearance Reciprocity requirements for personnel who hold National Security Clearances.

PSAMS shares with the Scattered Castles SCI database to facilitate National Security Clearance reciprocity, access to controlled facilities, and issuance of Personal Identify Verification (PIV) cards in support of HSPD-12:

- Clearance Eligibility Dates
- Personnel Type
- Organization
- Clearance/Access Level

- SCI Clearance certification dates including brief & debrief dates

## 5.3 How is the information transmitted or disclosed?

PSAMS data is transported via data exports and upload via secure system interfaces. Export and upload require human interaction with the system.

## 5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

No. Nevertheless, sharing of clearance data is legally mandated under Executive Order 12958 (as amended) for appropriate routine uses in accordance with Privacy Act law. An agreement is in place with the Intelligence Community regarding SCI information: PSAMS shares clearance eligibility dates, personnel type, organization, clearance level and SCI certification dates with the SCI database.

## 5.5 How is the shared information secured by the recipient?

OPM: Information is uploaded to the Clearance Verification System (CVS) data using OPM's "Extranet Service Portal" which is maintained and hosted by OPM's Federal Investigative Services Division (FISD). This information is hosted in a secure facility approved for storage of secure government data.

Intelligence Community: the Scattered Castles SCI database is hosted in a secure facility. Access to Scattered Castles is only possible via secure network.

Others will receive the information in a secured format.

## 5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

By executive order, in-depth training in the handling of clearance and privacy data is required. Personnel are required to sign an affidavit that they have been properly trained prior to handling this type of data.

## 5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

The privacy risk is that PII and in particular Social Security Number may be exposed and associated with an individual's name and date of birth as well as their clearance level and organization. The following are in place to mitigate the risk:

- There are no direct data interfaces: a person must generate an extract and transfer the data via secure transport method(s);
- Access to data is role-based;

- Personnel receive security training before being granted privileges to handle sensitive information.

# Section 6.0 Notice

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

In all cases, individuals are provided a notice required by the Privacy Act, 5 USC 552(a). The privacy statement, as required by the Privacy Act, 5 USC 552(a)(e)(3). states the reasons for collecting information, the consequences of failing to provide the requested information, and explains how the information is used. The collection, maintenance, and disclosure of information complies with the Privacy Act and the published System of Records Notice(s) (SORN) for the Office of Security records, Personal Identity Verification Management System (PIVMS) DHS-OS-002 System of Records Notice, 71 FR 53700, published September 12, 2006.

Individuals confirm presentation of and agreement with the Privacy Act Statement and agree to participate in the suitability and clearance process and submit to a named-based threat background check appropriate to job requirements.

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

Individuals who opt not to provide information cannot meet suitability requirements and are therefore ineligible for Federal service. Furthermore, they are ineligible to serve a role as a government contractor at a Federal facility for a period of more than six (6) months.

PSAMS stores clearance status and suitability information. Because it does not store assessments, there is no potential for derogatory information. There are therefore no special provisions for contesting PSAMS data.

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

Again, individuals may opt to not provide information; however, they can not meet suitability requirements and are therefore ineligible for Federal service. Individuals waive the right to choose how the information will be used on submission of the SF-85 or SF-86.

Individuals are notified of the uses of their information prior to collection. Once the information is given the individual has given consent to the uses. The DHS Security Office will not use the information outside of the scope of this PIA and the System of Records Notice. Should a new use for the information be foreseen the PIA and the SORN will be updated.

### 6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Individuals are provided notice of the information collection on the forms provided. Additionally, the System of Records Notice and this PIA provide additional notice of the collection, use, maintenance, and dissemination of the personally identifiable information.

## Section 7.0 Individual Access, Redress and Correction

### 7.1 What are the procedures which allow individuals to gain access to their own information?

PSAMS stores clearance process tracking information and the PII associated with the clearance record. The information is self-reported by the individual undergoing the clearance investigation when they submit their completed SF-85 / SF-86 or e-QIP entry. Individuals are able to correct erroneous information in e-QIP before submittal. Once that data has been submitted to PSAMS for suitability review and clearance processing by PSD, individuals must contact either PSD directly or go through Privacy Act/FOIA Office to gain access to their personally identifiable information.

Each Subject has the ability to address and provide mitigating information related to any derogatory information that is identified as part of his/her background investigation. Subjects are notified of any pending actions based on derogatory information and are provided a mechanism to provide information. If a derogatory finding is made, they have appeal rights, and also the ability to request information regarding their case via the DHS Freedom of Information Act (FOIA) office.

Contact information for the DHS FOIA Office is:
FOIA / PA D-3
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528.

### 7.2 What are the procedures for correcting erroneous information?

The information in PSAMS is obtained as a data extract from e-QIP from data provided directly by the individual. Accuracy of an individual's data is checked by an investigation; a PSD security assistant then reviews the results.

The specific procedures for an individual to view and request changes depend on the findings and the type of case. Subjects are notified in writing when DHS is prepared to make a derogatory finding based on the information at hand. The written notice advises the Subject of the mechanism for addressing the derogatory information.

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

The specific procedures depend on the findings and the type of case. Subjects are notified in writing when DHS is prepared to make a derogatory finding based on the information at hand.

The written notice advises the Subject of the mechanism for addressing the derogatory information. The individual will be notified based on a review of their response whether the derogatory information will be result in a change to their clearance status. If their clearance is suspended or revoked, they will be notified in writing and be provided with the specific information regarding their appeal rights and due process. Additionally instructions are provided on related security forms regarding changes or updates to data that may be required after submission.

### 7.4 If no redress is provided, are alternatives available?

Redress is provided.

### 7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

During initial security training, individuals are briefed to contact PSD regarding any personally identifiable information change requests. The individual can also contact security officers to make changes to their information. Other notifications and related processes are dependent on the type of case and specific findings as described above in section 7.1 and 7.2.

## Section 8.0 Technical Access and Security

### 8.1 Which user group(s) will have access to the system?

The daily access to PSAMS is granted to the appropriate Department employees and contractors involved in the investigation and adjudication of personnel suitability and clearances. This includes PSD, SSPD, and Human Capital. These individuals, by law and contract, are bound by the Privacy Act. Specific information about an individual will be shared with Department employees and its contractors who have a "need to know" regarding their vetting process. Department contractors are contractually obligated to comply with the Privacy Act in the handling, use and dissemination of all personal information.

More detailed access approval is documented in the PSAMS system administrative guide and in the System Security Plan documented in the system Certification and Accreditation documents. The high level information is provided below.

Account Request Guidelines:

The following access must be established prior to granting access to PSAMS:

a. DHS E-mail address.

b. Scope of information access required. Which is used to determine role based access to system data

c. Justification to support need for information access.

d. Approval official. This person must be able to validate the applicant's request for information access.

e. Approval date.

f. Adequate security suitability screening.

Access approval:

For Office of Security users: Roles and access is approved at the division chief or deputy division chief (or designated representative).

For non-Office of Security users, access is approved in the following manner: Access may be provided based on justified need and recommendation from Office of Security division chief.

Administrative access to PSAMS and the PSAMS database, and the associated administrative privileges, is granted to the Security Technical Integration & Support (STI&S) team, Office of Security, DHS.

## 8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Only contractors that provide direct support to Office of Security, Technical Support branch have access to the system. The contract vehicle includes the requirement that contractors sign a non-disclosure agreement and have completed security suitability screening for employment at DHS.

## 8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. Please see Answer provided in section 8.1.

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

PSAMS user accounts are individually approved by DHS Office of Security Division Chiefs before they are provisioned;

All users must have received DHS Computer Security training and have been vetted and cleared for access to privacy, sensitive and classified information; and,

Access to PSAMS is role-based: users of the system have access to a limited subset of data based on the concept of least privilege/limited access.

Procedures are documented in PSAMS Administrative Guide and PSAMS System Security Plan.

## 8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

The request is made by the user's supervisor and approved by their division chief. Roles are assigned based on the requirements of the job.

Procedures are documented in the PSAMS System Security Plan.

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

Auditing and technical safeguards include:

- A weekly review of security and application logs performed by the Information System Security Officer, reported to the Information System Security Manager;
- Monthly review of system usage reports;
- A quarterly assessment of audit findings.

## 8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All DHS employees and assigned contractor staff receive appropriate privacy and security training, and have undergone necessary background investigations and/or security clearances for access to sensitive, privacy or classified information or secured facilities. The DHS ensures this through legal agreements with its contractors and enforcement of internal procedures with all DHS entities involved in processing the background checks. Additionally, robust standard operating procedures and system user manuals describe in detail user roles, responsibilities and access privileges.

## 8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Certification & Accreditation for PSAMS was completed in September 2006.

## 8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

There is a residual privacy risk that PII and particularly SSN may be exposed and associated with an individual's name and date of birth as well as their clearance level and organization. The following are in place to mitigate the risk:

- Access to PSAMS requires a DHS domain account and requires that the user be logged into a DHS A LAN computer;
- PSAMS user accounts are individually approved by DHS Office of Security Division Chiefs before they are provisioned;
- All users have received DHS Computer Security training and have been vetted and cleared for access to privacy, sensitive and classified information;
- Access to PSAMS is role-based: users of the system have access to a limited subset of data based on the concept of least privilege/limited access;
- Write capability is limited to a few roles, is tracked and audited;
- External users are transmitted the least information possible;
- PSAMS has undergone review and met the Certification and Accreditation (C&A) criteria required of a system hosting privacy data.

# SECTION 9.0 TECHNOLOGY

## 9.1 Was the system built from the ground up or purchased and installed?

PSAMS was initially purchased as Government Off the Shelf (GOTS) software. Originally designed for use by ICE, the SARS system was purchased by DHS in 2004. It has since been customized for use by the DHS Office of Security.

## 9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Data integrity is enhanced by automated processes: information is shared between processes, minimizing user transcription errors. Privacy and security are enhanced by the granting of the least privileges possible to users. Data integrity issues and anomalies are minimized as a result of periodic reports & audits. Additionally, data is periodically uploaded to OPM Clearance Verification System (CVS) for integrity verification.

## 9.3 What design choices were made to enhance privacy?

The following are intended to enhance privacy:

- PSAMS utilizes a secure Oracle database as its backend data source;
- Access to PSAMS requires a DHS domain account and requires that the user be logged into a DHS A LAN computer;
- PSAMS user accounts are individually approved by DHS Office of Security Division Chiefs before they are provisioned;
- All users have received DHS Computer Security training and have been vetted and cleared for access to privacy, sensitive and classified information;

- Access to PSAMS is role-based: users of the system have access to a limited subset of data based on the concept of least privilege/limited access;
- Write capability is limited to a few roles, is tracked and audited;
- External users are transmitted the least information possible;
- PSAMS has undergone review and met the Certification and Accreditation (C&A) criteria required of a system hosting privacy data.

## CONCLUSION

The Personnel Security Activities Management System (PSAMS) automates tracking of the Personnel Security related activities at DHS headquarters. PSAMS serves as a mechanism for the electronic storage of tracking/completion dates of security checks, enhancing the ability of authorized personnel to retrieve information, and allowing reduction in the volume of paper documents. It is a repository for clearance and some privacy related data.

PSAMS uses as its backend a secure Oracle database. The PSAMS servers are hosted in a secure facility approved for the hosting of secure government systems. Access to PSAMS data is role-based according to the concepts of least privilege and limited access. PSAMS user accounts are individually approved by DHS Office of Security Division Chiefs before they are provisioned: all users have received DHS Computer Security training and have been vetted and cleared for access to privacy, sensitive and classified information. Write capability is limited to a few roles, is tracked and audited: external users are transmitted the least information possible.

## Responsible Officials

Project Manager:

John Pardun

Deputy Chief, Training and Operations Security Division

Office of Security

US Department of Homeland Security

## Approval Signature Page

Original signed and on file with DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security