OCC Security and Compliance Services: Privacy Impact Assessment (PIA)

Personnel Administration and Security System (PASS)

July 16, 2012

Version 2.0

Prepared by:
OCC Security and Compliance Services

Comptroller of the Currency
Administrator of National Banks
US Department of the Treasury

DOCUMENT CHANGE CONTROL

VERSION	DATE	SUMMARY OF CHANGES	NAME
2.0	07/16/2012	Update /Review of Document	Benjamin Eli/Pam Brown

Purpose

The Privacy Impact Assessment (PIA) is completed as a mandatory step in the certification and accreditation of IT systems, applications, and projects, that collect, process, store, and disseminate Personally Identifiable Information . The PIA examines the ways in which PII data are managed and protected by the target of evaluation.

NOTE

This document was prepared in support of the system's Certification and Accreditation effort. The document was developed in accordance with, or following the guidance contained in, the following:

- *The Privacy Act of 1974* (Public Law 92-132, 5 U.S. C. 552a).
- *Federal Information Security Management Act of 2002* (Title III of P.L. 107-347).
- Section 208 of the *E-Government Act of 2002* (Public Law 107-347, 44 U.S.C. Ch 36), April 17, 2003.
- Office of Management and Budget (OMB) Memorandum M-03-18, *Implementation Guidance for the E-Government Act of 2002*, August 1, 2003.
- OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003.
- OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, May 22, 2006.
- OMB Circular No. A-130**,** Revised, (Transmittal Memorandum No. 4)**:** *Management of Federal Information Resources*, 28 November 2000.
- Computer Matching and Privacy Act of 1988 (Public Law 100-503).
- Department of the Treasury Publication, TD P 25-05, *Privacy Impact Analysis Manual*, dated July 2006

Table of Contents

PRIVACY IMPACT ASSESSMENT

1. SYSTEM IDENTIFICATION

1.1. Name of System, Project, or Program:

Personnel Administration and Security System (PASS)

1.2. Responsible Organization

Critical Infrastructure Protection & Security (CIPS), Office of the Comptroller of the Currency (OCC), 250 E Street, Southwest Washington, DC 20219.

1.3. Information Contact(s)

Names of persons knowledgeable about the system, the system and data owner, security personnel, etc.

See PTA (Privacy Threshold Analysis) document.

1.4. Security Categorization

The system was assessed in its Security Categorization Report (SCR) as ***Moderate***, under guidance contained in Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, December 2003, as follows:

Information Type	**Confidentiality**	**Integrity**	**Availability**
Central Personnel Management	Moderate[1]	Low	Low
Personal Identity and Authentication	Moderate[2]	Moderate[3]	Moderate
Security Management	Moderate	Moderate	Low
Overall Per Category	**Moderate**	**Moderate**	**Moderate**
System Overall	**Moderate**		

1.5. System Operational Status

The System is currently Operational.

1.6. General Description/Purpose

The Personnel Administration and Security System (PASS) supports and automates personnel (i.e., employee and contractor) on-boarding, maintenance of personnel security information, and personnel off-boarding for the Office of the Comptroller of the Currency (OCC). The Critical Infrastructure Protection and Security (CIPS) office is OCC's personnel and physical security office. CIPS is the sponsoring business unit for PASS.

PASS improves OCC's ability to execute personnel security-related processes and manage personnel security-related data for employees and contractors throughout the employment life cycle. Additionally, PASS will help the OCC meets its requirements for physical access control and logical access control under Homeland Security Presidential Directive 12 (HSPD-12).

[1] *Special Factors Affecting Confidentiality Impact Determination*: Very sensitive information is typically personal information subject to the Privacy Act of 1974. (The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type.) Such information will often be assigned a ***moderate*** confidentiality impact level

[2] Where personal identity and authentication information is used in controlling access to facilities (e.g., Federal facilities, critical infrastructure facilities, key national assets) or for border control purposes, the consequences of unauthorized disclosure that permits credentials forgery can justify a ***high*** impact assignment.

[3] In the case of smaller organizations, and where the information affected is limited to employees, there will still be an impact, but the consequences may justify only a ***low*** provisional impact rating. Where a data modification permits access to facilities (or ingress into the United States) by individuals to whom access should be prohibited, the integrity impact could be ***high***.

1.7. Future Changes to PASS

Future releases of PASS include the capability for PASS to integrate with the OCC's system for electronic identity management, logical access control, and information technology provisioning, as well as OCC's emergency alert system. Additionally, PASS may ultimately be expanded to support and automate other physical security and emergency security business processes.

1.8. System Interconnection/Information Sharing

The following systems interact with PASS: HR Connect, Management and Accountability Reporting Tool ($MART), Microsoft Exchange, eDelivery Distributed Investigative File (DIF) Staging, ITS Remedy, Open Text, C*Cure, and the Employee Contact Information (ECI) Staging database.

HR Connect is external to the OCC.

2. PRIVACY IMPACT ASSESSMENT

2.1. Privacy Assessment

The following paragraphs detail the Privacy Assessment applicable to PASS.

2.1.1. Does this system collect any personal information in identifiable form about individuals?

Yes ☒ No □

2.1.2. Does the public have access to the system?

Yes □ No ☒

However, during the on-boarding process, contractors who do not yet have access to OCC IT systems will submit data about themselves to an instance of PASS that will be located outside the OCC firewall

2.1.3. Has a PIA been completed in the past?

Yes ☒ No □ N/A □

The initial PIA was completed in May 2011.

2.1.4. Has the existing PIA been reviewed within the last year?

Yes □ No ☒ N/A □

2.1.5. Have there been any changes to the system since the last PIA was performed?

Yes ☒ No □ N/A □

The OCC has implemented periodic maintenance releases to address system change requests and defects. However, these changes had no effect on the privacy posture of the system. Details about the changes are maintained in the Enterprise Change Control System.

2.2. Data in the System/Application

2.2.1. What elements of PII are collected, disseminated or maintained by the system?

- Name
- Date of birth
- Place of birth
- Social security number (SSN)
- Citizenship information
- Treasury Unique Identifier (TRUID)
- Person Identifier (Generated and maintained by the General Services Administration's (GSA) USAccess system)
- Home and work address information
- Home and work telephone information
- Home and work e-mail information
- Emergency contact information
- Supervisor name and TRUID
- HSPD-12 personal identity verification (PIV) data
- User principal name (UPN)
- FBI criminal check data and accompanying adjudication data
- Background investigation data and accompanying adjudication data
- HSPD-12 badge data (i.e., card holder unique ID [CHUID], card expiration date, federal agency smart credential number [FASCN])
- Photograph
- OCC credential data
- National security clearance data

2.2.2. Why is the information being collected?

PASS will collect the PII that is necessary to support OCC's personnel security business processes.

2.2.3. What are the sources of the information in the system?

Sources of the information supplied to PASS include the individual employee/contractor, Contracting Officer's Representatives (COR), Human Resources Specialists, Supervisors, CIPS personnel security staff, as well as information systems/organizations external to the OCC.

External information systems/organizations providing information to PASS include:

- HR Connect (Treasury's HR system)
- Office of Personnel Management's (OPM) Electronic Agency Delivery (eDelivery)

2.2.4. How will the data collected from sources other than Federal agency records or the individual be verified for accuracy?

Not Applicable. The PASS system does not collect data from any sources other than Federal agency records or the individual.

2.2.5. Who will have access to the data and how is access determined?

PASS will use role-based access control to control access to PII.

- Employees and contractors will have access to their own data.
- CORs and Contracting Officers (CO) will have access to data for contractors who are associated with contracts they administer. CORs and COs will not have access to date of birth, place of birth, and SSN data.
- HR Specialists will have access to data for all employees.
- Supervisors will have access to data for employees they supervise. Supervisors will not have access to date of birth, place of birth, and SSN data.
- CIPS personnel security staff will have access to data for all employees and contractors.

2.2.6. Describe the administrative and technological controls that are in place or that are planned to secure the information being collected.

The PASS system architecture and data is protected by the Network Infrastructure (NI) GSS. The NI GSS provides primary security services and data security mechanisms in support of OCC applications. These security services include identification and authentication (I&A), logical access controls, and auditing.

2.2.7. What opportunities will individuals have (if any) to decline to provide

information or to consent to particular uses of the information?

Individuals will be presented with a privacy statement and will be offered an opportunity to decline to provide data.

2.2.8. What is the life expectancy of the data and how will it be disposed of when it is no longer needed?

In accordance with the OCC 2010 Record Retention schedule Personnel Security files are destroyed upon notification of death or not later than 5 years after separation or transfer of employee or no later than 5 years after contract relationship expires, whichever is applicable.

2.2.9. Is the system owned, operated, and maintained by a contractor?

Yes □ No ☒

2.3. System of Records (SOR) Notice

Does the collection of this information require a new system of records under the Privacy Act (5 U.S.C. § 552a) or an alteration to an existing system of records?

Yes □ No ☒

2.4. Certification and Accreditation

Has the system been certified and accredited within the last three years?

Yes ☒ No □

Date ATO granted: May 2011.