$MART

(System, Management and Accountability Reporting Tools)

Privacy Impact Assessment (PIA)

Version 1.2

September 2010

Prepared by:

Information Risk Management

Comptroller of the Currency
Administrator of National Banks

US Department of the Treasury

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

Page

PRIVACY IMPACT ASSESSMENT

1. SYSTEM IDENTIFICATION

1.1 Name of System, Project, or Program:

The official system name:

$MART (System Management and Accountability Reporting)

1.2 Responsible Organization:

Office of the Chief Information Officer (OCIO)
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:

Key System Contacts (include name, phone, and email):

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:

Table 1-4: Security Categorization Summary

Information Type	Confidentiality	Integrity	Availability
Capital Planning	Low	Low	Low
Budget Execution	Low	Low	Low
Debt Collection	Moderate	Low	Low
User Fee Collection	Low	Low	Moderate
Official Information Dissemination	Low	Low	Low
Income	Moderate	Moderate	Moderate
Personal Identity and Authentication	Moderate	Moderate	Moderate
High Water Mark	**MODERATE**		
CATEGORIZATION	**MODERATE**		

1.5 System Operational Status

The current operational status of the $MART system is: Operational.

1.6 General Description/Purpose

$MART is a commercial off the shelf (COTS) application customized for the OCC and is based on PeopleSoft Financials. $MART is a web-based application, and is hosted in a client-server Windows environment. This application supports a variety of Financial Management (FM) functions including billing, general ledger, accounts payable, accounts receivable, asset tracking, depreciation, financial statements, budgeting, requisitions, procurement activities, reports, and commitment control. $MART reports vary by job function: accounts payable reports, budget reports, financial statements, accounts receivable reports, and asset management reports. $MART is conceptually displayed in Figure 1-1.

Technical details are on file.

Figure 1-1, $MART System Diagram

1.7 System Environment

The $MART application is located in and supported by the OCC Data Center. The Technical Assistance Center (TAC) serves as the national help desk for the OCC; it is physically co-located with the Data Center. Smoking, eating, and drinking are not allowed in the Computer Room except in an actual Shelter-in-Place situation. Emergency food and water are stored under the raised Data Center flooring

All personnel entering OCC facilities are required to wear an OCC-issued official badge. Full-time employees are issued an OCC Radio Frequency Identification (RFID) employee access badge and contractors are issued an OCC contractor badge. Visitors without an OCC badge are required to sign-in at the lobby security desk and show a government-issued ID such as a driver's license. A full-time OCC employee is required to sign-in the visitor at the security receptionist's desk and escort the visitor while inside the facility. Vendors delivering supplies or picking up backup tapes for storage at the off-site storage facility are authorized for limited areas within the Data Center and must show appropriate credentials to OCC security guards.

Physical access to the Data Center is controlled via keycard access. The Facility Security Officer can generate lists of personnel currently authorized for access to the Data Center.

Although all OCC workforce members are assigned facility keycard badges with picture ID on them, access to the Data Center must be specially authorized due to the sensitive nature of the work conducted in the Data Center.

1.8 Future Changes to $MART.

The financial systems application will be upgraded from version 8.4 to version 8.9 in January 2011.

1.9 System Interconnection/Information Sharing

$MART system interfaces play an important role in OCC daily business. Currently, there is a variety of interfaces. The $MART interfaces are:

Technical details are on file.

These interconnections are shown in the following figure.

Technical details are on file.

Figure 1-7, $MART Interconnections

2. PRIVACY IMPACT ASSESSMENT

2.1 Privacy Assessment

The following paragraphs detail the Privacy Assessment applicable to the ***$MART***.

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 ☑

2.1.3 Has a PIA been completed in the past?

Yes ☑ No ☐

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 ☐

2.2 Data in the System/Application

2.2.1 What elements of PII are collected and maintained by the system?

Information such as individuals' names, home addresses, and bank account numbers (for purposes of direct deposit) are held within $MART.

2.2.2 Why is the information is being collected?

Required by Financial Management Services for payment.

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

All information is collected via OCC personnel records and via the interfaces described above.

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

Some Privacy information is received from the banks. Per MOUs/ISAs, the banks have the responsibility for establishing the accuracy of information they supply and for proper formatting the transmittal to $MART. $MART then checks for format errors and then loads into the database.

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

Only the OCC's Accounting Office staff has access to $MART data and access is determined based on each individual's job role. A user's request for a $MART data access role must be approved by that individual's supervisor. There is a predefined set of access roles for which specific access permissions are allocated.

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

All management, operational, and technical controls in place and planned for $MART are described in the System Security Plan, which must be approved in writing by various $MART management officials.

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 have ability to decline providing privacy information at the system entry points which are: TERS, Citibank and SATO. These entry points have the responsibility to provide the individual with the opportunity to decline providing information. If they do not decline at the entry system, then $MART will use the privacy information where needed. No other opportunities are provided by $MART for declining.

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

The current life expectancy of the data is currently 7 years. Once the size reaches a point where disposition must be addressed, then $MART will dispose of information in agreement with federal regulation for financial information.

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: **June 7, 2010**