

**U.S. Department of the Treasury
Office of the Comptroller of the
Currency**

Privacy Impact Assessment

*Version 2.2
2007*

Prepared by:

Office of the Comptroller of the Currency
Department of the Treasury
Independence SQ
250 E St. SW
Washington, DC 20219-0001

Controlled By: Jackie Fletcher

Controlling Office: Chief Information Officer

Accreditation Date: March 31, 2007

Re-Accreditation Date: March 31, 2010

WARNING

This document belongs to the Department of the Treasury, Office of the Comptroller of the Currency (OCC), Office of the Chief Information Officer (OCIO), Information Technology Network Infrastructure General Support System (GSS). It may not be released without the express permission of the OCIO. Refer requests and inquiries for the document to Dave Smith, Information System Security Officer (ISSO), at (301)324-3233 or at Dave.Smith@occ.treas.gov. (re: TD P 15-71, Chapter III, Section 23)

SENSITIVE BUT UNCLASSIFIED

Privacy Impact Assessment
Version 2.2
March 20, 2007

NOTE


This document was prepared in support of System Certification and Accreditation following the guidance contained in:

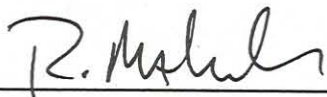
- *The Privacy Act of 1974* (Public Law 92-132, 5 U.S. C. 552a).
- *Federal Information Security Management Act of 2002* (Title III of P.L. 107-347).
- Section 208 of the *E-Government Act of 2002* (Public Law 107-347, 44 U.S.C. Ch 36), April 17, 2003.
- Office of Management and Budget (OMB) Memorandum M-03-18, *Implementation Guidance for the E-Government Act of 2002*, August 1, 2003.
- Office of Management and Budget (OMB) Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003.
- Office of Management and Budget (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

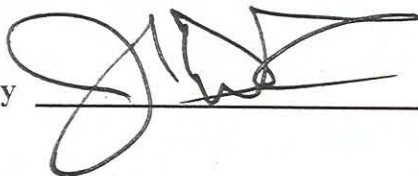
Record of Changes				
Version Number	Date Released	Description of Changes	Pages Affected	Changes Made By
1.0	02/14/2007	Initial Working Draft	All	SAIC
2.0	03/05/2007	Second draft – FISMA System Privacy Threshold Analysis Determination Checklist section 2.1 added	All	SAIC
2.1	03/06/2007	Correction of minor errata	All	SAIC
2.2	03/20/2007	Incorporated comments and suggestions Updated SORN section	All	SAIC

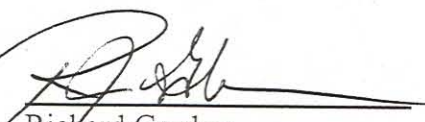
REVIEW AND APPROVAL SIGNATURES

The SMART Privacy Impact Assessment was prepared for the exclusive use in support of the Certification and Accreditation Program. The plan has been reviewed and approved at the responsible office, the Information Systems Security Officer, the Chief Information Officer, and at the Privacy Advocate level.

Reviewed by:  Date: 5-7-07
Rick Armwood
Smart Information System Security Officer (ISSO)

Reviewed by  Date: 5-18-07
Roger Mahach
Chief Information Security Officer

Reviewed by  Date: 5-18-07
Jim Devlin
Chief Privacy Officer

Approved by:  Date: 5/16/07
Richard Gordon
Deputy Chief Information Officer


Approved by:  Date: 5/18/07
Jackie Fletcher
Chief Information Officer

TABLE OF CONTENTS

1.	SYSTEM IDENTIFICATION.....	1
1.1	System Name/Title.....	1
1.2	Responsible Organization.....	1
1.3	Information Contact(s).....	1
1.4	Security Categorization.....	2
1.5	System Operational Status.....	2
1.6	General Description/Purpose.....	2
1.6.1	Production Platform.....	3
1.6.2	Development Platform.....	5
1.6.3	Reporting Platform.....	6
1.6.4	Production Support Platform.....	8
1.6.5	Windows 2003 Platform.....	8
1.6.6	Software.....	10
1.7	System Environment.....	10
1.8	System Interconnection/Information Sharing.....	11
2.	PRIVACY IMPACT ASSESSMENT.....	14
2.1	Privacy Assessment.....	14
2.2	Data in the System/Application.....	14
2.3	System of Records Notice (SORN).....	16
2.4	SORN Impact Evaluation.....	16

LIST OF FIGURES

Figure 1-1:	SMART System Diagram.....	3
Figure 1-2:	SMART Production Platform.....	4
Figure 1-3:	SMART Development Platform.....	5
Figure 1-4:	SMART Reporting Platform.....	7
Figure 1-5:	SMART Production Support Platform.....	8
Figure 1-6:	SMART Windows 2003 Platform.....	9
Figure 1-7:	SMART Interconnections.....	13

1. SYSTEM IDENTIFICATION

1.1 System Name/Title

The official system name is: \$SMART. The Commercial Off-the-Shelf (COTS) product name is PeopleSoft Financials version 8.4.

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 20219-0001

1.3 Information Contact(s)

See Table 1-1 – 1.3, Contact Information for \$SMART. Name of person(s) knowledgeable about, or the owner of, the system:

Table 1-1: System Owner Contact Information for \$SMART

System Owner	
Name:	Tom Marcou
Title:	Director, Accounting
Address:	250 E Street, Southwest Washington, DC 20219-0001
Phone:	(202) 874-4997
E-mail:	tom.marcou@occ.treas.gov

Table 1-2: Privacy Officer Contact Information for \$SMART

Privacy Officer	
Name:	Jim Devlin
Title:	Chief Privacy Officer
Address:	250 E Street, SW Washington, DC 20219-0001
Phone:	202-874-5013
E-mail:	jim.devlin@occ.treas.gov

Table 1-3: Information System Security Officer (ISSO) Contact Information for SMART

Information System Security Officer (ISSO)	
Name:	Jason Teller
Title:	SMART ISSO
Address:	250 E Street, SW Washington, DC 20219-0001
Phone:	(202) 874-3809
E-mail:	Jason.Teller.@occ.treas.gov

1.4 Security Categorization

The System is assessed for Security Categorization under the 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

SECURITY CATEGORIZATION SUMMARY			
Components	Impact Assessment		
	Confidentiality	Integrity	Availability
Corrective Action	Low	Low	Low
Budget Formulation	Low	Low	Low
Capital Planning	Low	Low	Low
Budget Execution	Low	Low	Low
Management Improvement	Low	Low	Low
Debt Collection	Moderate	Low	Low
User Fee Collection	Low	Low	Moderate
Official Information Dissemination	Low	Low	Low
Congressional Liaison	Moderate	Low	Low
Central Records & Statistics Management	Moderate	Low	Low
Income	Moderate	Moderate	Moderate
Personal Identity and Authentication	Moderate	Moderate	Moderate
High Water Mark	Moderate	Moderate	Moderate
CATEGORIZATION	Moderate		

1.5 System Operational Status

The System is currently “Operational” because it is in the Operations & Maintenance Phase of the System Development Life Cycle (SDLC).

1.6 General Description/Purpose

SMART is a COTS application customized for the OCC and is based on PeopleSoft Financials version 8.4. SMART is hosted on a Windows 2003 Server General Support System (GSS) platform with database tables maintained in Microsoft SQL Server 2000

and its associated Relational Database Management System (RDBMS). 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. SMART reports vary by job function: accounts payable reports, budget reports, financial statements, accounts receivable reports, and asset management reports. SMART source code is stored internally on the SQL database server and externally in directories on the server. All source code, interface code, and code changes are stored in PVCS with changes occurring every few months. SMART does 15 minute incremental backups and then ships the data off-site every 15 minutes. SMART is conceptually displayed below.

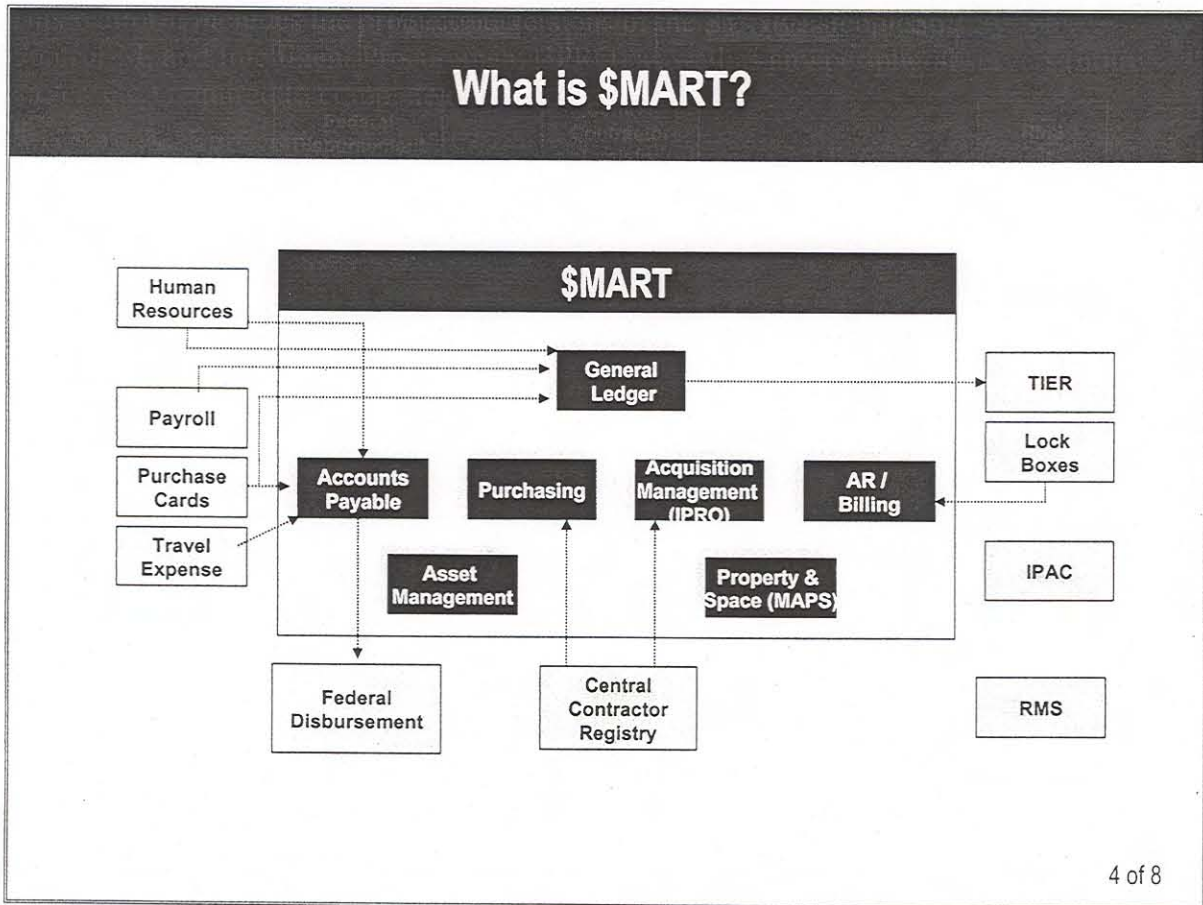


Figure 1-1: SMART System Diagram

1.6.1 Production Platform

The production platform is utilized by FM to conduct official OCC financial transactions. This platform includes the production versions of the SMART PeopleSoft System, Control-M, and Intelligent Procurement (IPRO) as well as any peripheral servers (utility server, etc.) required to complete daily transactions.

TECHNICAL DETAILS ARE ON HAND

NOTES:

The Windows 2003 PeopleSoft database server (HQSQLPSFIND03) hosts this SMART environment: OCPF84W3 – Windows 2003 test environment. The MS-Office/nVision scheduler server (HQAPPSFIND06) provides the software and processing needed to access nVision via the web. The OCC LDAP (OCCAD01) server, not pictured, connects with all other servers on the network. It maintains user IDs and passwords for access across the network.

1.6.2 → 1.6.5 Redacted Technical Details

1.6.6 Software

The Windows 2003 platform is the used for testing the compatibility of SMART-related applications with the Microsoft Windows 2003 operating system. This platform will eventually become the production platform after OCC makes a full transition to the Windows 2003 operating system. The following are the primary software components necessary for performing SMART processing. Note: The system does not employ Public Key Infrastructure (PKI), Voice over Internet Protocol (VoIP), mobile code, spam or spyware protection, collaborative computing, or outsourced security services.

- **Operating Systems.** Windows 2003 is run on both primary and backup servers. Windows XP is run on client machines.
- **Applications.** The application used in the SMART system is the PeopleSoft Financials COTS product. It has not been modified in any way for use in the OCC environment.

1.7 System Environment

The SMART system operates within the secure confines of the Data Center located within the OCC facility at 835 Brightseat Road, Landover, MD. 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 (Iron Mountain) 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. When setting up authorization for a new employee or a full-time, on-site contractor, the Facility Security Officer makes a determination as to which access profile is appropriate to the new employee or contractor's job role. In the case of a contractor, the Facility Security Officer is notified by the Contracting Officer Technical Representative (COTR) several weeks before the end date of the contract that the contract will be ending and that the people associated with it will need to be removed from the keycard access system. For special cases such as when a contractor working on a special project needs access to the Data Center for a limited period of time such as a few weeks, the contractor's sponsor must complete the Physical Access Control System Request Form. A form must be completed for each person. The Facility Security Officer receives a Remedy system trouble ticket requesting that their physical access be deleted if the person is to be terminated or updated in the case of a personnel transfer. The Facility Security Officer is the designated official who reviews and approves the access list and authorization credentials at least annually.

1.8 System Interconnection/Information Sharing

The SMART system provides the following interconnections with other information technology services.

- National Finance Center (NFC) Payroll Interface loads OCC payroll data from a flat file into the PS_OCC_ACCTG_LINE record using a custom SQR program.
- Citibank NA (original purchase) Interface loads employees' purchase card data into the Accounts Payable (AP) module. This process includes two SQR processes run sequentially as part of a batch job and then the delivered Voucher Build program will create the vouchers from the staging tables.
- Citibank RA (reallocation allowance) Interface is a custom SQR program that loads reallocation data for previously loaded purchase card transactions into two staging tables. The data is then moved to the PeopleSoft General Ledger by the Journal Generator process.
- Travel and Expense Reporting System (TERS) Interface loads employee's travel expense data into the AP module. The process reformats the received flat file and places the data in staging tables. Two SQR processes are executed sequentially as part of a batched job, and then the delivered Voucher Build program will create the vouchers from the staging tables.
- Central Contractor Registry (CCR) Vendor Interface loads external vendor information from the Department of Defense's Central Contractor Registry system into the PeopleSoft vendor tables.
- Tier Interface is a custom SQR program that creates a simple export file from monthly reporting data in the General Ledger. The file is sent to the Department of Treasury as part of the month-end close process.
- ECS/EFT Interface is a series of delivered programs, commonly referred to as the "pay cycle," that creates export files with outgoing payment data. These files are then sent to Financial Management Service (FMS), which processes the payments on the OCC's behalf.

- TERS E-mail Interface is a custom SQR program that creates a simple export file of daily employee expense payments that are being reimbursed. The flat file is run through a program that automatically generates emails that notify these employees that they are being reimbursed the noted amounts.
- IPRO Interface loads data from PeopleSoft's Purchasing module to SAP's IPRO contract management software using a custom SQR program in PeopleSoft to load a staging table, and then an executable file run by the Control-M batch scheduler to load the data into IPRO. After the file has been worked, the information is interfaced back to a second staging table from IPRO using an executable file run by the Control-M batch scheduler and then to the PeopleSoft Purchasing module by a custom SQR program in PeopleSoft.
- 1099 Tax/Internal Revenue Service (IRS) Interface is a series of delivered programs that create an export file with OCC's yearly withholding information for payments. This file is sent to the IRS electronically.
- Charter Bank Interface is a custom SQR program that loads customer data from the CAIS system at OCC into the delivered PeopleSoft AR customer tables.
- Employee Vendor Interface loads employee vendor information from the HR Connect human resources system into the PeopleSoft vendor tables.
- Department/Org Interface uses a custom SQR program to load department information from HR-Connect human resources system into the PeopleSoft department control table. If the data already exists, no updates/inserts are performed.
- Location code Interface uses a custom SQR program to load information from the HR Connect human resources system into the PeopleSoft location control tables. If the data already exists, no update/inserts are performed.
- Aperture Interface uses custom SQR programs to load asset information from the PeopleSoft Asset Management tables into the Aperture space management software on a separate server and vice versa. If the last modification took place in Aperture, then the PeopleSoft AM tables are updated. If the last modification took place in the PeopleSoft AM tables, then the Aperture tables are updated.

SMART maintains a variety of interconnections using Control-M to establish a peer-to-peer temporary connection. Connections to IPRO, CCR, Citibank, and TERS are established through batch-mode processes through Control-M. These interconnections are shown in the following figure.

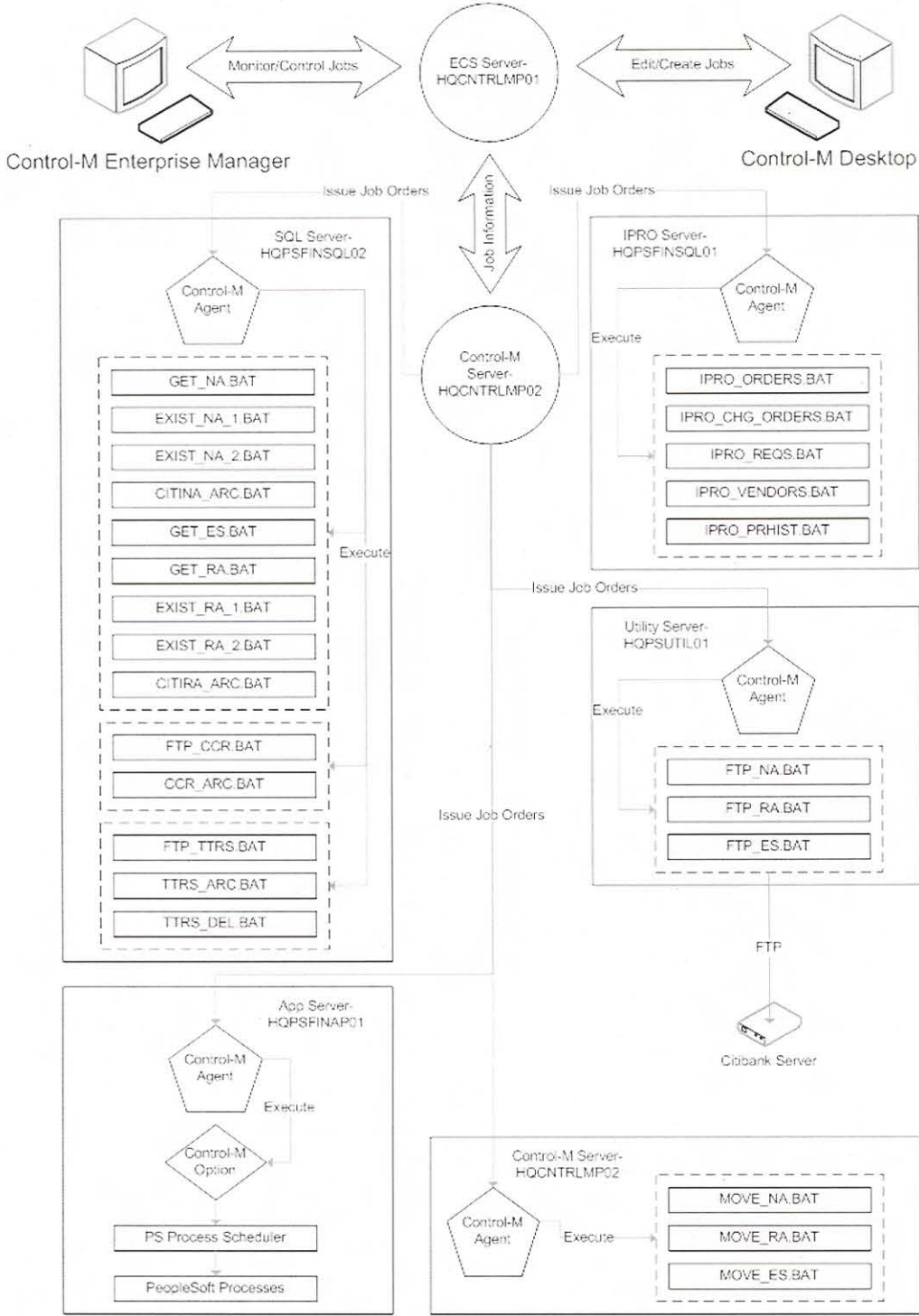


Figure 1-7: SMART Interconnections

2. PRIVACY IMPACT ASSESSMENT

2.1 Privacy Assessment

The following paragraphs detail the Privacy Assessment applicable to the SMART MA.

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

Y N

2.1.2 Does the public have access to the system?

No, SMART is not a publicly accessible system.

2.1.3 Has a PIA been done before?

Y N

This is the initial PIA for the SMART system.

2.1.4 Has it been at least three years since the last PIA was performed?

Y N Has a Privacy Impact Assessment been completed?

Not Applicable. This is the initial PIA for the SMART system.

2.1.5 Has the system changed since the last PIA was performed?

Y N

Not Applicable. This is the initial PIA for the SMART system.

2.2 Data in the System/Application

2.2.1 Describe the information to be collected, why the information is being collected, the intended use of the information, and with whom the information will be shared.

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

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

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

2.2.3 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 the information they supply and for proper formatting for transmittal to SMART. SMART then checks for format errors and then loads into the database.

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

Only the OCC's Accounting Office staff have access to SMART data and access is determined based on each individual's job role. A user's request for a SMART 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.

2.2.5 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 SMART are described in the System Security Plan, which must be approved in writing by various SMART management officials.

2.2.6 What opportunities will individuals have (if any) to decline to provide information or to consent to particular uses of the information?

Individuals have the ability to decline providing privacy information at the system entry points which are: the banks, TERS, and e-Time. 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 SMART will use the privacy information where needed. No other opportunities are provided by SMART for declining.

2.2.7 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 the life of the system. Once the size reaches a point where disposition must be addressed, then SMART will dispose of information IAW federal regulations for financial information.

2.3 System of Records Notice (SORN)

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?

Y N

Office of Management and Budget (MB) Circular A-130, *Management of Federal Information Resources* (Revised) (Transmittal Memorandum No. 4), December 2000, Appendix I, paragraph 4c (1) details which actions that may require a new or altered SORN.

2.4 SORN Impact Evaluation

The SMART system is not covered by one or more of the following SORNs, as published in the Federal Register / Vol. 70, No. 131 / Monday, July 11, 2005 / Notices. This notice covers all systems of records adopted by the OCC up to June 21, 2005. It includes:

- CC .100—Enforcement Action Report System
- CC .110—Reports of Suspicious Activities
- CC .120—Bank Fraud Information System
- CC .200—Chain Banking Organizations System
- CC .210—Bank Securities Dealers System
- CC .220—Section 914 Tracking System
- CC .340—Access Control System
- CC .500—Chief Counsel’s Management Information System
- CC .510—Litigation Information System
- CC .600—Consumer Complaint and Inquiry Information System
- CC .700—Correspondence Tracking System

The following *SORN Impact Evaluation Summary*, details the evaluation of the stated criteria in order to determine if a new or altered SORN is required in support of the OCC’s SMART Major Application. Any criteria marked with an “x” in the “Yes” column would indicate the likelihood of a new or altered SORN Report being required. Although Table 2-1 does not indicate that the system’s functionality or configuration has changed, a new SORN would be required for SMART because it had not been designated as a Major Application previously.

Table 2-1: SORN Impact Evaluation Summary

SORN Impact Evaluation Summary OCC SMART Major Application		
Criteria (OMB Circular A-130, Appendix I, paragraph 4c(1))	Evaluation	
	Yes*	No
1. A significant increase in the number, type, or category of individuals about whom records are maintained.		X
2. A change that expands the type or categories of information maintained.		X
3. A change that alters the purpose for which the information is used.		X
4. A change to equipment configurations (either hardware or software) that creates substantially greater access to the records in the system of records.		X
* Note: All "Yes" answers must be supported in detail		