Financial Management Service

Privacy Impact Assessment

The Financial Management Service (FMS) Mission is to provide central payment services to Federal Program Agencies, operate the federal government's collections and deposit systems, provide government-wide accounting and reporting services, and manage the collection of delinquent debt owed to the government.

FMS Privacy Impact Assessments (PIA) http://www.fms.treas.gov/pia.html

Document Date: **May 23, 2011**

Name of System/Application: **Surety Information Management System (SIMS IV)**

System Overview:

SIMS IV, a minor system, is an automated storage and processing computer system for supporting the FMS Surety Bond Branch (SBB) in administering the Surety Bond Program. The legal basis for the SBB program stems from Public Law Title 31, USC 9304-9308, which authorizes the acceptance of corporate surety companies on bonds running to the United States. The Secretary of the Treasury has delegated the responsibility for administering the Federal Surety Bond Program to the Financial Management Service (FMS), who in turn established the SBB to carry out the function. Companies that wish to direct-write Federal bonds, reinsure Federal bonds, or be recognized as Admitted Reinsurers must apply and be approved by FMS.

SIMS IV is a Java 2 Platform Enterprise Edition (J2EE) web-based application on a WebSphere Application Server (WAS) accessible from the FMS Insider Page. The SIMS IV servers and databases reside on the Regatta Complex located at the Hyattsville Regional Operations Center with no interconnections to other systems. All data for the system resides in a DB2 database on the Regatta.

System of Records Notice (SORN): **.009 Treasury Financial Management Systems**

SYSTEM APPLICATION/GENERAL INFORMATION:

1) **Does this system contain any personal information about individuals?**

   a. Is the information about individual members of the public? YES

   b. Is the information about employees or contractors? NO

DATA in the SYSTEM:

1) **Categories of individuals covered in the system**
   Check all that apply:
   __ Employees
   __ Contractors
   __ Taxpayers
   _X_ Others (describe)—Insurance company officials

2) **Identify the sources of information in the system**
   Check all that apply:
   __ Employee

__ **Public**
__ **Federal agencies**
__ **State and local agencies**
_X_ **Third party sources (Insurance Company Officers)**

a. What Federal agencies are providing data for use in the system? Not applicable

b. What State and local agencies are providing data for use in the system? None

c. From what other third party sources will data be collected? None

d. What information will be collected from employees or contractors? None

e. What information will be collected from the public? None

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than FMS records be verified for accuracy? Manually and automatically
b. How will data be checked for completeness? Manually
c. What steps or procedures are taken to ensure the data is current and not out-of-date? Auditor reads data.

d. In what document(s) are the data elements described in detail? Refer to applicable sections of the project documentation, i.e., SIMS IV System Security Plan, SIMS IV System Contingency Plan

ATTRIBUTES OF THE DATA:

1) How is the use of the data both relevant and necessary to the purpose for which the system is being designed? The financial statements are loaded in for review.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed? No

3) Will the new data be placed in the individual's record? Not applicable

4) Can the system make determinations about employees or members of the public that would not be possible without the new data? Not applicable

5) How will the new data be verified for relevance and accuracy? Not applicable

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use? Not applicable

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? (Explain.) Not applicable

8) How will the data be retrieved? (If personal identifiers are used to retrieve information on the individual, explain and list the identifiers that will be used to retrieve data.) Not applicable

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them? None

10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent.) Not applicable

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

What are the retention periods of data in this system? How long will the reports produced be kept? In accordance with the National Archives and Records Administration (NARA) schedule for the records related to this system (**data** will be retained in SIMS IV for seven (7) years. Currently, any FMS records that are proposed for destruction must be approved in advance, and in writing, by the FMS Assistant Commissioner for Management and the FMS Chief Counsel, to ensure compliance with NARA disposition schedules and any record retention orders to which FMS is subject. The FMS Chief Counsel outlined this process in a memorandum to the FMS Assistant Commissioners, dated March 7, 2000.

1) What are the procedures for disposition of the data at the end of the retention period? Where are the disposition procedures documented? This is discussed above.

2) If the system is operated in more than one site, how will consistent use of the system and data be maintained at all sites? Not applicable.

3) Is the system using technologies in ways that the FMS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? No

4) How does the use of this technology affect employee or public privacy? Not applicable

5) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain. Internal users of the system may access data with the use of a unique UserID and password.

6) What kinds of information are collected as a function of the monitoring of individuals? An audit trail will be captured for each transaction that adds, deletes or modifies any information. The audit trail will include the UserID of the person performing the transaction.

7) What controls will be used to prevent unauthorized monitoring? Access to the audit logs is limited to authorized individuals within the Information Resources (IR) **organization. Requests for review of the data must come from management-level personnel**

ACCESS TO DATA:

1) **Who will have access to the data in the system?**
Check all that apply:

_ Contractors
_X _ Users
_X_ Managers
_X_ System administrators
_X_ System developers
__X Others (explain) _____Data will be accessible by the SIMS IV staff, the SIMS IV database administrator at FMS, and by certain IR Development Staff and authorized contractors working in IR.

2) **How is access to the data by a user determined?** Are criteria, procedures, controls, and responsibilities regarding access documented? SIMS IV defines access control policy, groups and individual user permissions based on least privilege. Access and permissions are restricted to the approved domain. Granting of initial or change in access or permissions must be accomplished in writing and approved by the Surety Bond Branch Manager, through ITIM.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.** User access will be restricted. Internal users will have the level of access needed to perform their duties. Users with administrative privileges are restricted to the minimum necessary and all action are monitored and recorded in various system logs and audit trails.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)** The SIMS IV application contains an access control module. Users are defined in an LDAP user directory. Roles have been defined and are used to grant access to each individual commensurate with the user's need. Specific roles have been defined for administrators, Manager, Acting Manager, Clerical, Auditor, who need to enter specific transactions in SIMS IV. Active auditing of system and application access and the use of individual UserIDs allow enforcement of individual accountability and traceability of user actions. Rules of Behavior are signed by users before gaining access to the system.

5) **If contractors are/will be involved with the design, development or maintenance of the system were Privacy Act contract clauses inserted in their contracts and were other regulatory measures addressed?** Not Applicable

6) **Do other systems share data or have access to the data in the system?**

__yes
_X_no

If yes,

a. Explain the interface. None

b. Identify the role responsible for protecting the privacy rights of the public and employees affected by the interface. Not applicable

7) Will other agencies share data or have access to the data in this system?

__yes
_X_no

If yes,

a. Check all that apply:

__Federal
__State
__ Local
__Other (explain) _____FPAs including Dept. of Justice_____

b. Explain how the data will be used by the other agencies.

c. Identify the role responsible for assuring proper use of the data.

FMS Privacy Impact Assessments (PIA) http://www.fms.treas.gov/pia.html