US Department of the Treasury
Financial Management Service
Financial Operations
Financial Accounting and Services Division
Surety Bond Branch
Surety Information Management System (SIMS IV)
Privacy Impact Assessment (PIA)

Name of Project: Surety Information Management System (SIMS IV)
Bureau: Financial Management Service (FMS)
Financial Operations (FO)
Financial Accounting and Services Division (FASD)
Surety Bond Branch (SBB)

A. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals? Yes

a. Is this information identifiable to the individual[1]?

Yes

b. Is the information about individual members of the public?

Yes

c. Is the information about employees?

Yes

2)

3) What is the purpose of the system/application?

The SIMS IV is a mid-tier ("TIER III") mission supportive application system on the FMS internal web-based intranet designed to support the FMS Surety

[1] "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

Bond Branch ("SBB") in administering the Surety Bond Program. SIMS IV will be used by the SBB to perform quarterly and annual reviews, process new applications, re-certify approximately 350 insurance companies each year, and publish a list of Treasury Certified companies in Treasury Circular 570.

4) What legal authority authorizes the purchase or development of this system/application?

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.

B. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

Members of the public.

2) What are the sources of the information in the system?

Insurance companies submit financial statement data on diskettes or Compact Disk ("CD"), as well as correspondence and related hard copy documents (i.e., National Association of Insurance Commissioners (NAIC) Biographical Affidavits for individual officers and directors of the insurance companies, which contain personal information.) The names of key officers and directors are imbedded as electronic fields within the diskette or CD submissions made by the insurance companies.

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

The source of personal corporate officer or director information can be either from the direct submissions made by insurance companies in the form of diskettes or CDs, or from hard copy NAIC Biographical Affidavits prepared by the individual and forwarded to the SBB through the insurance company. In the case of the latter, certain types of personal identifiers (specifically, names and social security numbers of key officers and directors) would then be manually inputted by the SBB auditor into SIMS IV.

b. What Federal agencies are providing data for use in the system?
None

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

d. From what other third party sources is the data collected? Accounting and actuarial companies.

e. What information will be collected from the employee and the public?

As previously noted in items C. 2) and C. 2) a. above, the names of key corporate officers and directors are obtained by insurance companies and

contained in paper copy form in NAIC Biographical Affidavits which are submitted to the SBB for key officers and directors. In addition, these affidavits contain other types of personal identifiers (i.e., address, social security number, marital status and other information.) Only certain names and social security numbers of key officers and directors are manually inputted by the SBB auditor into SIMS IV. Hard copy information sources are secured in cabinets located in a locked file room.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than FMS records be verified for accuracy?

The data collected from insurance companies in the form of electronic submissions via diskette and CD can only be cross-checked for matching purposes to hard copy sources (i.e., NAIC Biographical Affidavit for the personal identifiers of name and social security number for key officers and directors.) This is no "verification" for accuracy, per se, since the SBB cannot check the names and social security numbers to actual social security documents.

b. How will data be checked for completeness? SBB auditors review NAIC Biographical Affidavits for completeness and responsiveness to the questions asked.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

The names and social security numbers of key officers and directors residing in SIMS IV is kept current. As changes occur based upon the submission of either quarterly or annual diskettes, CDs and hard copy financial statements from the insurance company, the SBB auditor requests that NAIC Biographical Affidavits for applicable individuals be filed. The names and social security numbers of new key officers and directors are then manually inputted into SIMS IV by an SBB auditor.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

Refer to applicable sections of the Surety Bond Branch SIMS IV Functional and Data Requirements Document and the SIMS IV Configuration Management Plan Document for this information.

C. ATTRIBUTES OF THE DATA:

1) **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?** The use of the data is relevant and necessary. SBB has to make determinations, in applications by companies to become Treasury Certified, as to the acceptability of company officers and or directors. The data provides a means to prior work experience, name change of the individual and the reasons thereof, outstanding litigation or enforcement matters, suspension or revocation of professional, occupational or vocational licenses or permits, disciplinary actions, criminal offenses or civil offenses, cease and desist actions and other informational areas of regulatory concern.

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?** Not Applicable

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

4) **Can the system make determinations about employees/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 is the data to be retrieved?** Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data is **not** maintained nor retrieved by means of a personal identifier. Information can be retrieved in SIMS IV by insurance company name, NAIC company number and NAIC group code number.

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 individuals can grant consent.**

There are no opportunities

D. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?** Not Applicable

2) **What are the retention periods of data in this system?**

In accordance with the National Archives and Records Administration (NARA) schedule for the records related to this system, data submissions received by insurance companies on diskettes, CDs or via the internet, as well as electronic versions of auditors' worksheets and notepads, are retained in SIMS for six (6) years. Electronic copies of system output, such as reports, are destroyed or deleted when no longer needed for current business.

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

Annually, the SBB, in conjunction with the FO Privacy Act Liaison, arrange for the boxing and inventory identification of insurance company data sources and SIMS records for shipment to the Federal Records Center (FRC.) The SBB prepares inventory records schedules for FO's Records Administrator

which itemize and specify the record being transmitted to the FRC. After the FRC receives delivery of these records, the procedures for subsequent disposition of the data at the end of the applicable retention periods are dictated and implemented by NARA. See item E. 2) above.

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

5) **How does the use of this technology affect public/employee privacy?** Not Applicable

6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

   SIMS IV does **not** have the capability to locate by way of a "search" function any individual, nor can it monitor individuals. SIMS IV does contain personal identifiers (names and social security numbers) for certain key insurance company officers and directors as part of data tables residing in the system.

7) **What kinds of information are collected as a function of the monitoring of individuals?** Not Applicable

8) **What controls will be used to prevent unauthorized monitoring?** - An application audit trail records user's activities on SIMS IV data. Audit trails exist within the database to log changes to tables of Certification History, Deduction History, and PHS History. The information that is tracked includes the user ID, Role, Insurance Company, Date, Time, Transaction, Field/Record Changed and Description.

9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

   System of Records Notice 009, dated August 2005.

10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.** Not Applicable.

E. ACCESS TO DATA:

1) **Who will have access to the data in the system?** (E.g., contractors, users, managers, system administrators, developers, tribes, other)

Data contained in SIMS IV will be accessible by the SBB staff, the SIMS IV Database Administrator, certain IR Development staff and FMS 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 uses several associated components contained within the general support system ("GSS") located at the FMS HROC facility. The GSS components provide both functionality and some security services for SIMS IV, and contain sensitive data in the form of privileged SIMS IV account passwords and UserIDs needed for system development and management functions.

SIMS IV users complete a *Rules of Behavior* form and are then granted access to SIMS IV from the Database Administrator upon request made by the SBB Manager. Users are given a unique login identification name and then set a unique password. Both items are required for login. Bi-monthly, the SIMS System Administrator provides the SIMS Information Systems Security Official ("ISSO") with a written log of login attempts made for the period, both authorized and unauthorized. The ISSO would review the log to determine whether there are any concerns related to login activity for the period warranting further follow-up or action.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

The SIMS IV application access control is enforced at the GSS and operating system level by forcing the user to provide a username and password to gain initial access to the system. The SIMS IV application requires a separate username and password, provided thru WebSphere, to log in and use the system. WebSphere will authenticate these credentials against the LDAP directory.

The SIMS IV system uses MS Windows authentication to gain access to the GSS. The Application Manager determines the roles for all users of SIMS IV.

FMS generally ensures that all user IDs belong to currently authorized users. Identification data is kept current by adding new users and deleting former users through the Enterprise Security Access Administration Service (ESAAS) system.

The role of a user determines the user's access and type of access. A user of the SIMS IV system can be assigned as an Auditor, Senior Auditor, Manager, Acting Manager, System Administrator (SA), or Clerk. These roles have different privilege

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) GSS components provides security services for SIMS IV through account passwords and UserIDs. SIMS IV users complete a *Rules of Behavior* form prior to being granted access to the database by the SIMS IV Database Administrator upon a request by the SBB Manager. Bi-monthly, the SIMS System Administrator provides the ISSO with a written log of login attempts made for the period, both authorized and unauthorized. The ISSO would review the log to determine whether there are any concerns related to login activity for the period warranting further follow-up or action.

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

6) **Do other systems share data or have access to the data in the system? If yes, explain.** No

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?** The System Owner, System Manager, and ISSO share responsibility in protecting the personal data when it is shared between the systems.

8) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?** No

9) **How will the data be used by the other agency?** Not Applicable

10) **Who is responsible for assuring proper use of the data?** The Manager, Surety Bond Branch and the SBB Information System Security Officer (ISSO) and/or the Alternate ISSO.