



The Bureau of the Fiscal Service

Privacy Impact Assessment

The mission of the Bureau of the Fiscal Service (Fiscal Service) is to promote the financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, payments, and shared services.

This Privacy Impact Assessment (PIA) is a public document and will be made available to the general public via the Fiscal Service PIA webpage (shown below).

Fiscal Service - Privacy Impact Assessments (PIA):

http://www.fiscal.treasury.gov/fsreports/fspia/fs_pia.htm

Name of System: Surety Information Management System (SIMS IV)

Document Version: 1.0

Document Date: 02/19/2015

SYSTEM GENERAL INFORMATION:

1) System Overview: Describe the purpose of the system.

SIMS IV is a supportive application system on the Fiscal Service internal web-based intranet designed to support the Fiscal Service Surety Bond Section (SBS) in administering the Surety Bond Program. SIMS IV will be used by the SBS to perform quarterly and annual reviews, process new applications, recertify approximately 350 insurance companies each year, and publish a list of Treasury Certified companies in Treasury Circular 570.

2) Under which Privacy Act Systems of Records Notice (SORN) does the system operate? Provide number and name.

Not applicable (N/A); the records in SIMS IV are not retrieved by personal identifier.

3) If the system is being modified, will the SORN require amendment or revision?

yes, explain.

no

4) Does this system contain any personal information about individuals?

yes

no

a. Is the information about members of the public?

Yes

b. Is the information about employees or contractors?

No

5) What legal authority authorizes the purchase or development of this system?

The legal basis for the Federal Surety Bond 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 Fiscal Service, who in turn established the SBS 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 Fiscal Service.

DATA in the SYSTEM:

1) Identify the category of individuals in the system

Check all that apply:

Employees

Contractors

Taxpayers

Others (describe) Insurance companies/insurance executives

2) Identify the sources of information in the system

Check all that apply:

Employee

Public

Federal agencies

State and local agencies

***Third party (insurance companies)**

a. What information will be collected from employees or contractors?

None

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

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

d. What state and local agencies are providing data for use in the system? None

e. From what other third party sources will data be collected? insurance companies

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources, other than Fiscal Service records, be verified for accuracy? N/A—SIMS IV is an analytical tool.

b. How will data be checked for completeness? SBS auditors review National Association of Insurance Commissioners (NAIC) Biographical Affidavits for completeness and responsiveness to the questions asked.

c. What steps or procedures are taken to ensure the data is current?

The names and titles of key officers are 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 SBS auditor requests that NAIC Biographical Affidavits for applicable individuals be filed. The updated information is then manually inputted into SIMS IV by an SBS auditor.

d In what document(s) are the data elements described in detail?

Refer to applicable sections of the project documentation, i.e., SIMS IV Functional and Data Requirements Document and the SIMS IV Configuration Management 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 use of the data is relevant and necessary. SBS has to make determinations in applications by companies to become Treasury Certified, as to the acceptability of company officers and or directors.

- 2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? How will this be maintained and filed?** No. The system will not derive new data or create previously unavailable data.

- 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.)**

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

- 9) **What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

SIMS IV does not provide the capability to produce reports on individuals.

- 10) **What opportunities do individuals have to decline to provide information (i.e., in such cases where providing information is voluntary) or to consent to particular**

uses of the information (other than required or authorized uses)? How can individuals grant consent?

Participation in the Surety Bond program will not be approved if requested information is not provided.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) 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 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 IV for 7 years. Electronic copies of system output, such as reports, are destroyed or deleted when no longer needed for current business. Any Fiscal Service records that are proposed for destruction must be approved in advance, and in writing, by the Fiscal Service Assistant Commissioner for Management and the Fiscal Service Chief Counsel, to ensure compliance with NARA disposition schedules and any record retention orders to which Fiscal Service is subject.

2) What are the procedures for disposition of the data at the end of the retention period? Where are the disposition procedures documented?

Annually, the SBS arranges for the boxing and inventory identification of insurance company data sources and SIMS IV records for shipment to the Federal Records Center (FRC.) The SBS prepares inventory records schedules 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 2 in Maintenance and Administrative Controls Section above.

3) 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

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

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

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain. No. The system does not provide the capability to identify, locate, and monitor individuals.

7) What kind of information is 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 users' activities on SIMS IV data. Audit trails exist within the database to log changes to table 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.

ACCESS TO DATA:

1) Who will have access to the data in the system?

Check all that apply:

Contractors

Users

Managers

System Administrators

System Developers

Others (explain) _____

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. Criteria, procedures, controls, and responsibilities regarding access are documented.

SIMS IV users must read and agree to a *Rules of Behavior* document prior to receiving access. Once completed, the SBS Supervisor requests access for the user which is subsequently granted by the dataset administrator. Users can use either uid/pw or PIV. Access and permissions are restricted to the approved domain. Users are given a unique login identification name and then set a unique password. Both items are required for login. Granting of initial or change in access or permissions must be accomplished in writing and approved by the SBS Supervisor.

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 to the level of access needed to perform their duties. Users with administrative privileges are restricted to the minimum access necessary. All actions are monitored and recorded in a weekly log 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)

SIMS IV access is role-based. 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 SBS Supervisor. Weekly, the ISSO reviews an audit log of login attempts made for the period, both authorized and unauthorized. The ISSO reviews the log to determine whether there are any concerns related to login activity for the period, and if the concerns warrant further follow-up or action.

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. SIMS IV was internally developed.

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

_yes
_X_no

If yes,

a. Explain the interface.

Not applicable

b. Identify the role responsible for protecting the privacy rights of the public and employees affected by the interface. Not applicable. SIMS IV does not share data or interface with any other systems.

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

yes
 no

If yes,

a. Check all that apply:

Federal
 State
 Local
 Other (explain) Insurance companies

b. Explain how the data will be used by the other agencies. Not applicable

c. Identify the role responsible for assuring proper use of the data. System Owner and ISSO.