

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

*Privacy Impact Assessment
Supervisory Information System - Examiner
View (EV)*

*Version 1.0
February 20, 2008*

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

Controlled By: Chief Information Security Officer
Controlling Office: IT Security Office
Control Date: September 30, 2007
Decontrol On: Indefinitely


******* OCC Sensitive Security Information*******


The information contained herein was produced, in whole or in part, by the Department of the Treasury, Office of the Comptroller of the Currency (OCC) for the benefit of the Department of the Treasury, OCC. As such, this information is the sole, proprietary, and exclusive property of OCC. Therefore, this information may only be used by (1) OCC, without limitation, (2) employees and agents whose access is necessary, and limited to, the accomplishment of the project tasks, and (3) any other individual or agency granted access by OCC under separate authority. All information contained herein is OCC Sensitive Security Information whether such information is in written, graphic, electronic, or physical form. Those granted access to the information by clause (2) or (3) above will hold these materials and information in strict confidence. Access and use of this information by any other entity or individual are strictly prohibited. Should you have any questions about the proper use or access to this information contained herein, please contact OCC's Chief Information Security Officer, Roger Mahach, at (202) 874-7276 for instructions.


SIS-EV Privacy Impact Assessment Record of Changes				
Version No.	Date Released	Description of Change	Pages Affected	Changes Made By
1.0	September 30, 2007	Initial publication.	All	IT Security Office

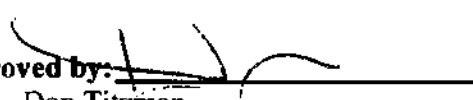
REVIEW AND APPROVAL SIGNATURES

The SIS-EV 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: 3/5/08
Dave Woodson
Information System Security Officer (ISSO)

Reviewed by:  Date: 3/5/08
Roger Mahach
Chief Information Security Officer

Reviewed by:  Date: 3/5/08
Gayle Rucker
Chief Privacy Officer

Approved by:  Date: 3/4/08
Don Titzman
Director, Supervisory Information


Approved by:  Date: 3/07/08
Bajinder Paul
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.....	3
1.6	General Description/Purpose.....	3
1.6.1	Production Platform.....	7
1.6.2	Software.....	9
1.7	System Environment.....	10
1.8	System Interconnection/Information Sharing.....	10
2	PRIVACY IMPACT ASSESSMENT	12
2.1	Privacy Assessment.....	12
2.2	Data in the System/Application.....	12
2.3	System of Records Notice (SORN).....	15
2.4	SORN Impact Evaluation.....	15

LIST OF FIGURES

Figure 1	SIS-EV Distributed Application Architecture.....	Error! Bookmark not defined.
Figure 2	Existing SIS Distributed Application Architecture.....	Error! Bookmark not defined.

LIST OF TABLES

Table 1-1:	System Owner Contact Information for SIS-EV.....	1
Table 1-2:	Privacy Officer Contact Information for SIS-EV.....	1
Table 1-3:	Information System Security Officer (ISSO) Contact Information for SIS-EV.....	2
Table 1-4:	Security Categorization Summary.....	2
Table 2-1:	SORN Impact Evaluation Summary.....	16

1 SYSTEM IDENTIFICATION

1.1 System Name/Title

The official system name is: Supervisory Information System – Examiner View (SIS-EV).

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 SIS-EV. Name of person(s) knowledgeable about, or the owner of, the system:

Table 1-1: System Owner Contact Information for SIS-EV

System Owner	
Name:	Don Titzman
Title:	Director, Midsize/Community Bank Supervision
Address:	Office of Midsize/Community Bank Supervision
Phone:	(202) 874-4429
E-mail:	don.titzman@occ.treas.gov

Table 1-2: Privacy Officer Contact Information for SIS-EV

Privacy Officer	
Name:	Gayle Rucker
Title:	Chief Privacy Officer
Address:	250 E Street, SW Washington, DC 20219-0001
Phone:	202-874-1023
E-mail:	gayle.rucker@occ.treas.gov

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

Information System Security Officer (ISSO)	
Name:	Dave Woodson
Title:	Information System Security Officer
Address:	250 E Street, SW Washington, DC 20219-0001
Phone:	202-874-2101
E-mail:	dave.woodson@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

Information Type	Confidentiality	Integrity	Availability
Corrective Action	Low	Low	Low
Program Evaluation	Low	Low	Low
Program Monitoring	Low	Low	Low
Policy and Guidance Development	Low	Low	Low
Management Improvement	Low	Low	Low
Official Information Dissemination	Low	Low	Low
Reporting and Information	Low	Moderate	Low
IT Security	Low	Moderate	Low
Business and Industry Development	Low	Low	Low
Financial Sector Oversight	Moderate	Low	Low
Judicial Hearings	Moderate	Low	Low
Legal Defense	Moderate	Moderate	Low
Legal Investigation	Moderate	Moderate	Moderate
Legal Prosecution/ Litigation	Low	Moderate	Low
Resolution Facilitation	Moderate	Low	Low
Inspections and Auditing	Moderate	Moderate	Low
Standards Setting/Reporting Guideline Development	Low	Low	Low
Overall Per Category	Moderate	Moderate	Moderate

Information Type	Confidentiality	Integrity	Availability
System Overall	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

SIS-EV is a software application designed by the OCC to assist bank examiners in preparing and conducting supervisory activities for financial institutions. It is part of the SIS suite of software that supports the work efforts of OCC bank examiners and management personnel. SIS-EV, which is a Windows .Net application, is used to support the Assistant Deputy Comptrollers (ADCs) and Field Office Analysts in the management of the institutions and bank examiners assigned to their office.

SIS-EV is a client-server application that can be used in a continuously connected manner or in a stand-alone, disconnected manner. This is to allow examiners to use the program while in bank examinations without a network connection. . In order to maximize the level of “code re-use” for the SIS applications, an architecture that supports both on-line and off-line applications has been implemented. All SIS-EV servers and users’ computers are connected to the OCC intranet inside of a firewall, except in the case of incoming Virtual Private Network (VPN) connections. The standard OCC VPN solution is used. The OCC VPN solution is used by remote users to replicate the data they have entered into their database remotely into the servers housed at the OCC data center.

The SIS-EV application provides the following.

- It is an on-line and off-line application to support the Supervisory Office users.
- The application allows single data entry by the users and stores the data in the SIS database repository so that the data can be shared with others. SIS-EV will share the same SIS databases used by SIS-Large Banks Institutional Database (LBID) and SIS-Reports.
- SIS-EV shares the same code base as other SIS applications to save on development and maintenance costs.
- Eventually, SIS-EV must handle a large amount of document data, such as Work Papers, Reports of Examination, Comments, etc., in a very efficient manner (i.e.,

reduce transactions in a document intensive replicated environment by providing last update replication with compression).

- SIS-EV must provide On-line Transaction Management, which is the coordination of data transactions being entered by on-line users, off-line users, and batch jobs.

The design will divide the system into these five layers of discreet physical components: Presentation, Business Façade, Business Rules, Data Access Layer, and Database. Through inter-process communication between these components via .NET Remoting, SIS-EV shall have a framework and a single code base that can support connected functionality.

The Presentation tier will be a smart client Windows Forms application rather than a Web browser based client. All access to data is done through a Façade. The Presentation tier should never directly access Business Rule Objects (BROs), Data Access Objects (DAOs), or the database. Communication across the system boundary has some performance issues, and Façade access should be limited to one to three calls per page.

The Business Façade acts as a middleman between the Presentation and the Business objects. It reduces the number of calls that WinForm needs to make to the Business objects. It does this by retrieving data on behalf of the WinForm and aggregating or packaging the data in a single DataSet, then returning the DataSet to the WinForm as a return value or throws as exception.

The Business Rules layer is made up of BROs, which perform complex tasks such as data processing; aggregation; transactions across multiple records, tables, or databases; and data validation. BROs are responsible for data validation and performing operations across multiple tables or data sources. BROs are also responsible for managing transactions. Because a Business Rule may need to update more than one table, the BROs are responsible for creating, committing, or rolling back transactions. A "Transaction" object that encapsulates the connection and transaction functionality will be exposed to the Business Rule layer to manage transactions.

The Data Access layer act as an abstraction layer to the database and are used to retrieve and update data from a data source and return the data to the application in a more "developer friendly" format. This layer hides most of the complexity of database access from the application developer. The DAOs should be the only objects that access the database directly. Transactions and connections are created via a custom object at the Business Rule layer and passed into each DAO. DAOs should perform very simple database access (select, update, delete, and insert) and only update single tables or tightly-related tables. They can also perform simple data validation and type conversion. DAOs inherit from the base Data Access class.

SIS-EV is a client-server application. Users shall use the application via OCC's internal Local Area Network (LAN), Wide Area Network (WAN), dial-up, or VPN, or in a stand-alone setting with a local copy of the database replicated to the user's computer. There is no encryption of data transmissions provided, except for the OCC's standard VPN solution. The "Windows Integrated Login" on IIS and the Sybase ASA database are enabled to provide tightly integrated authentication between the operating system (Windows Server 2003) and the web (IIS 6.0) and database servers (Sybase ASA). This provides a single login capability for the users.

Only the application architects, Database Administrators (DBAs), and other authorized operations staff have membership to the Administrators group and console access to the SIS-EV servers. Developers may be granted the Administrator rights to the development, preview, or maintenance servers on an as-needed basis. Remote access is granted to the architects and DBAs to perform remote production supports. The .NET Framework's Code Access Security is used to implement a security mechanism to manage permission to the application.

SIS-Admin is a web-based "back office support" application that provides numerous administration screens used to maintain SIS-EV user and LBID user data, as well as other reference data that is part of the SIS-EV and LBID applications. A variety of users have access to some or all SIS-Admin modules, including Help Desk personnel, Customer Service Representatives, Large Bank system administrators, Examiner View support examiners, and Examiner View technical staff members. The SIS-Admin application is an OCC internal-use-only tool accessible from the OCC intranet.

SIS-Admin is composed of the modules listed below. Depending on a user's level of authorization, he or she may or may not be able to view or access all of these modules.

- The Help Desk area is used to investigate SIS-EV user problems with institution subscriptions, replication, and more. Several types of users have access to the Help Desk area, including the IT Services Technical Assistance Center (TAC), Customer Service Representatives, SIS-EV support examiners, and the SIS-EV development team.
- The EV Administration area allows users with Supervisory Office authority to make corrections to certain SIS-EV production data. Administrators have full access to this area to perform additional functions as required.
- The Examiner View Reference Data area allows users to maintain the reference data that is used in SIS-EV, which includes data that defines all of the exam types and their related modules and procedures.

- The Large Bank Administration area allows authorized users to modify Large Bank production data in order to maintain the Large Bank institution hierarchies, maintain web links to external information and surveys, and to add a new survey. Access to this area of SIS-Admin is restricted to the LBID system administrators only.

The Large Bank Reference Data area allows users to maintain the reference data that is used in LBID, which includes the data that defines all of the Products, Rating Concerns, and Top Concerns. Access to this area of SIS-Admin is restricted to the Large Bank system administrators only.

- The SIS Reference Data area allows users to maintain the reference data that is used in both LBID and SIS-EV. For example, the Industry Codes that control the SIS-EV Credit Concentrations are also used for the Large Bank Industry Exposure definition in LBID. Other examples include Law Cites, MSA Codes, and Office Addresses. Access to this area of SIS-Admin is restricted to the LBID system administrators and SIS-EV support examiners only.
- The System Administration area is primarily used by the SIS architects to solve replication and extract problems and to monitor system services.
- The Reports area in SIS-Admin is primarily used by the SIS architects and developers to research problems related to database extracts and replication, and to view audit logs and reports.
- The Technology Service Providers area allows users to view Technology Service Provider data. Authorized users can also update or add a Technology Service Provider into the list of institutions supervised by the OCC.
- The User Admin and Security area allows authorized users to add and maintain SIS-EV user profiles, LBID user and security profiles, and SIS-Admin security profiles. Access to this area of SIS-Admin is restricted to the LBID system administrators and SIS-EV support examiners only.
- The Security Definitions area is primarily used by the SIS architects and developers to maintain LBID and SIS-Admin database security objects and collections.

The SIS-Reports software tool that allows users to create reports on both SIS-EV data and LBID data. It gives the user the ability to run a variety of reports for the SIS suite of applications. The reports generated in SIS-Reports are used to supervise banks. The reports can be used by: the Supervisory Office, the ADC, the ADC Analyst, the Examiner in Charge (EIC), Licensing, Special Supervision, and other users throughout the OCC. The SIS-Reports application gets its data from the SIS-EV and LBID databases. The

SIS-Reports database stores historical data (by quarter for SIS-EV and by month for LBID) as well as current data. SIS-Reports also contains reports that are accessed directly by other applications. SIS-National Resource Planning Tool (NRPT), SIS-EV, and SIS-Peer Analytical Data (PAD) are examples where those applications directly access and display reports developed by the SIS Reports team.

The SIS-Reports architecture consists of three layers. The database contains both current and historic data for LBID, SIS-EV, and SIS-National credit Tool (NCT). There is a middle-tier Jaguar server where the business logic and report code are stored. Finally, the client application is installed on the user's machine and is primarily responsible for allowing the user to choose a report and displaying the end results of the report.

SECTION 1.6 TECHNICAL DETAILS ARE AVILABLE AND ON FILE

SECTION 1.6 TECHNICAL DETAILS ARE AVAILABLE AND ON FILE

1.7 System Environment

The Data Center is the facility that directly supports the SIS-EV application. 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. 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

SIS-EV provides files to the Federal Reserve Bank (FRB) and Federal Deposit Insurance Corporation (FDIC) twice per month. Memoranda of Agreement (MOAs) between the OCC and the FRB and FDIC were examined as part of the Network Infrastructure (NI) General Support System (GSS) since they were written at the agency level, rather than the application level. There is a receive-only connection from SIS-EV to the OCC's

mainframe and to other SIS applications. The SIS-Admin and SIS-Reports tools are used by other SIS applications besides SIS-EV.

2 PRIVACY IMPACT ASSESSMENT

2.1 Privacy Assessment

The following paragraphs detail the Privacy Assessment applicable to SIS-EV.

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, SIS-EV is not a publicly accessible system.

2.1.3 Has a PIA been done before?

Y N

This is the initial PIA for the SIS-EV 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 SIS-EV 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 SIS-EV 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.

The primary business function is the acquisition and recordation of results of supervisory review of financial institution activities. All examination data (Reports of Examination, Comments, work papers) and some reference data are stored for each District's data repository. Districts include mid-size and credit card institutions as well as Large Banks.

In addition to examination data, examiners can input financial institution characteristics such as supervisory history or institution profile that might contain bank contacts or institution owners. The system lets the examiner conduct an examination while being disconnected from the OCC network and then upload and synchronize the data from the examiner's laptop to the databases. There is a receive-only connection from SIS-EV to the OCC's mainframe and to other SIS applications.

SIS-EV provides files to the FRB and FDIC twice per month.

Information maintained in this system is used by the OCC to carry out its statutory and other regulatory responsibilities, including other reviews of the qualifications and fitness of individuals who propose to become responsible for the business operations of OCC-regulated entities.

While the application does not specifically collect, maintain, or share PII information, users have the ability to attach documents to the system to support the findings reached and recorded by the users. There is no physical limitation on the format or content of the information that can be attached as work papers. The information can include documents, spreadsheets, presentation materials, and images obtained through scanning. The information that is attached can be generated by OCC employees, or could be information provided by non-OCC employees, such as bankers and data processing service providers.

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

SIS-EV stores data from all community bank districts, mid-size and credit card institutions, and large banks and handles a large amount of document data, such as Work Papers, Reports of Examination, Comments, etc. The information gathered is part of the bank examination process, examiners' work papers, and the final examination reports.

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

Checks made for business types of data received or processed are addressed at the application level. The SIS-EV application does not perform input validity and authentication checks per se but it allows input only from drop-down menus and preformatted data fields. Comments sections are the only free-form fields for which input is accepted. The Supervisory Office also reviews information periodically using a manual process so that any incorrect data that might be found would get corrected. Data is replicated via the OCC LAN or the agency's approved high-speed VPN service. There is a reset button available to users that prevents replication if the user thinks he or she has taken erroneous or unintentional actions

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

The application determines the user's account and group information and then verifies the account/group against security tables in the database to determine if the user is authorized to access the page.

The role to which a user is assigned determines the types of functionality to which that user will have access. Security is set for every page in the application. If the SIS-EV administrator does not specifically allow a user access to a certain field or menu option, that option is grayed out for that user and nothing will happen if the user clicks on a gray area. The application is menu-driven. Only the SIS-EV administrator (and administrators for other SIS applications and defined user groups) can use the SIS-Admin tool.

The EV Administration area allows users with Supervisory Office authority to make corrections to certain SIS-EV production data. Administrators have full access to this area to perform additional functions as required.

Only the application architects, Database Administrators (DBAs), and other authorized operations staff have membership to the Administrators group and console access to the SIS-EV servers. Developers may be granted the Administrator rights to the development, preview, or maintenance servers on an as-needed basis. Remote access is granted to the architects and DBAs to perform remote production supports. The .NET Framework's Code Access Security is used to implement a security mechanism to manage permission to the application.

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 SIS-EV are described in the System Security Plan, which must be approved in writing by various SIS-EV 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 institutions. These entry points have the responsibility to provide the individual with the opportunity to decline providing information. No other opportunities are provided by SIS-EV 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 SIS-EV 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 SIS-EV system is 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 SIS-EV 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.

Table 2-1: SORN Impact Evaluation Summary

SORN Impact Evaluation Summary OCC SIS-EV Application CC .100—Enforcement Action Report System		
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.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2. A change that expands the type or categories of information maintained.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3. A change that alters the purpose for which the information is used.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4. A change to equipment configurations (either hardware or software) that creates substantially greater access to the records in the system of records.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
* Note: All “Yes” answers must be supported in detail		