



# **BSA IT Modernization**

**Infrastructure, Portal, Identity Management, Security  
General Support System (IRIS GSS)  
Privacy Impact Assessment (PIA)**

Version 1.4

Final

May 03, 2011

---



## Revision History

Change Record				
Revision Number	Document ID	Description of Change	Change Effective Date	Change Entered By
0.1	Privacy Impact Assessment Project E V0.1	Draft PIA version for Identity Management, Access Control and Web Portal	Jan-04-2010	Rahul Marwaha
1.0	Privacy Impact Assessment RUP_IDM V1.0	Final	Jan-22-2010	Rahul Marwaha
1.1	Privacy Impact Assessment IRIS V1.1	Privacy Act Officer is Changed to Privacy Officer, Name of the document	Jan-24-2011	Rahul Marwaha
1.4	PIA 1.4	Updated sections E.9, E.10 per Privacy Official.	May 3, 2011	Quentin Robinson

---

## Table of Contents

- 1. Privacy Impact Assessment IRIS .....4
  - A. CONTACT INFORMATION ..... 4
  - B. SYSTEM APPLICATION/GENERAL INFORMATION..... 5
  - C. DATA IN THE SYSTEM..... 6
  - D. ATTRIBUTES OF THE DATA ..... 7
  - E. MAINTENANCE AND ADMINISTRATIVE CONTROLS..... 9
  - F. ACCESS TO DATA..... 10

## 1. Privacy Impact Assessment Template

Name of Project: BSA IT Modernization  
 Bureau: Financial Crimes Enforcement Network (FinCEN)  
 Project's Unique ID:  
 Name of the system: IRIS GSS  
 Unique System Identifier: 015-04-01-12-01-1018-00

### A. CONTACT INFORMATION

- 1) Who is the person completing this document? (Name, title, organization and contact information).  
 Name: Rahul Marwaha  
 Organization: Deloitte  
 Email: [Rahul.Marwaha@fincen.gov](mailto:Rahul.Marwaha@fincen.gov)
  
- 2) Who is the system owner? (Name, organization and contact information).  
 Name: Jim Dykes  
 Organization: FinCEN  
 Email: [jim.dykes@fincen.gov](mailto:jim.dykes@fincen.gov)
  
- 3) Who is the system manager for this system or application? (Name, organization, and contact information).  
 Name: Gerard Lamerton  
 Organization: FinCEN  
 Email: [gerard.lamerton@fincen.gov](mailto:gerard.lamerton@fincen.gov)
  
- 4) Who is the IT Security Manager who reviewed this document? (Name, organization, and contact information).  
 Name: Quentin Robinson  
 Organization: FinCEN  
 Email: [Quentin.Robinson@fincen.gov](mailto:Quentin.Robinson@fincen.gov)
  
- 5) Who is the Bureau/Office Privacy Officer who reviewed this document? (Name, organization, and contact information).  
 Name: Gayle Rucker  
 Organization: FinCEN  
 Email: [Gayle.Rucker@fincen.gov](mailto:Gayle.Rucker@fincen.gov)
  
- 6) Has organizational privacy management information previously been provided with another PIA?  
 Yes  No  N/A  Enclosed Reference  
 Details\* \_\_\_\_\_
  
- 7) If so, has any of this information changed since the previous PIA was submitted? If NO, please provide the title & date of the previous PIA and proceed to Section B of the questionnaire.

Yes  Partial  No  N/A  Enclosed Reference  
 Details\* \_\_\_\_\_

8) Who is the Reviewing Official?

Director, FinCEN  
 P.O. Box 39, Vienna, VA 22183-0039  
 E-mail: [InfoAssure@fincen.gov](mailto:InfoAssure@fincen.gov)

**B. SYSTEM APPLICATION/GENERAL INFORMATION**

1) Does this system contain any information about individuals?

*Individual* - means a citizen of the United States or an alien lawfully admitted for permanent residence.

Yes  Partial  No  N/A  Enclosed Reference

Details\* The system collects the following information:

- Individual / Organization Name
- Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN) or Employer Identification Number (EIN)
- Address including ZIP Code
- Date Of Birth
- Supervisor
- Supervisor Title
- Supervisor Phone
- Supervisor E-mail
- BSA Direct Web Based Training status
- Agency and/or Agency Memorandum of Understanding (MOU) group
- Bank Account including Routing Number
- Amount and type of Transaction

a. Is this information identifiable to the individual<sup>11</sup>?

Yes. Information is collected, maintained, or used that is identifiable to the individual in the system.

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

Yes.

c. Is this information about employees?

Yes

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

The IRIS GSS comprises the Identity Management System (IDM), Access Control Management (ACM) and Registered User Portal (RUP) portions. The IDM is a centralized identity provisioning and administration solution that automates the process of adding, updating, deleting, and synchronizing user account information from applications and directories.

The ACM System secures applications by providing centralized authentication, authorization and auditing to enable single sign-on and secure access control.

<sup>11</sup> "Identifiable Form" - 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).

The RUP provides a secure unified access point in the form of a web-based user interface for non-employees who have permissions to access data in the BSA IT Mod systems.

**3) What legal authority authorizes the purchase or development of this System/ application?**

The Department of the Treasury is authorized to “establish and maintain operating procedures with respect to the government-wide data access service and the financial crimes communications center maintained by FinCEN.” These procedures may provide, among other things “for the coordinated and efficient transmittal of information to, entry of information into, and withdrawal of information from, the data maintenance system maintained by FinCEN,” and “appropriate standards and guidelines for determining ... who is to be given access to the information maintained by FinCEN [and] what limits are to be imposed on the use of such information[.]” 31 U.S.C. § 310(c)(1), (2)(A), (2)(B).

The information contained in BSA databases, access to which is mediated by the use of information in the IRIS GSS, is collected under the authority of the Bank Secrecy Act, the popular name for Titles I and II of Public Law 91-508, as amended, and codified at 12 U.S.C. § 1829b, 12 U.S.C. §§ 1951-1959, and 31 U.S.C. §§ 5311-5331. The regulations implementing the authority contained in the Bank Secrecy Act are found at 31 C.F.R. Part 103. The authority to administer 31 C.F.R. Part 103 has been delegated to FinCEN.

**C. DATA IN THE SYSTEM**

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

Within the scope of Release 1, the IDM and the RUP will cover external users from law enforcement, financial regulatory, intelligence community as well as certain financial institutions. The ACM system will support both FinCEN internal and external users.

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

**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?**

Yes  Partial  No  N/A  Enclosed Reference

Details\* The external user will register using an online application form. FinCEN currently uses Microsoft Active Directory to house internal user information.

**b. Will Federal agencies provide data for use in the system?**

Yes  Partial  No  N/A  Enclosed Reference

Details\* The agency coordinator will provide background investigation information.

**c. Will Tribal, State and local agencies provide data for use in the system?**

Yes  Partial  No  N/A  Enclosed Reference

Details\* The agency coordinator will provide background investigation information.

**d. Will data be collected from other third party sources?**

Yes  Partial  No  N/A  Enclosed Reference

Details\*

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

The IDM system will collect the following information from employees -

- Name
- Addresses
- Contact Information
- Organization Information
- Supervisor Information
- Challenge Questions

3) Accuracy, Timeliness, and Reliability

The Privacy Act of 1974 requires that agencies only maintain data that is accurate, relevant, timely, and complete about individuals. These requirements are statutory and need to be addressed.

a. How will data collected from sources other than FinCEN records are verified for accuracy?

Details: The registered user approval process, from which this information is collected, includes a verification step that is performed by a designated person, an agency coordinator, within the external agency. This person will be responsible for verifying the identity of the agency user.

b. How will data be checked for completeness?

Data type validations are performed to ensure the data is complete and accurate. The system will have relevant error-checking and form validation functionality. The register process includes a three step approval process. Data is checked for completeness and accuracy for each one of these steps.

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).

Yes Partial No N/A Enclosed Reference

Details\* The registered user approval process, from which this information is collected, includes a verification step that is performed by a designated person, an agency coordinator, within the external agency. This person will ensure the data used to verify an agency user's identity is the most current.

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

Yes Partial No N/A Enclosed Reference

Details\*Design specification report will cover the data elements in detail.

D. 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?

Yes Partial No N/A Enclosed Reference

Details\* Refer section B and question 2.



- 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?  
Yes Partial No N/A Enclosed Reference  
 Details\*
- 3) Will the new data be placed in the individual's record?  
Yes Partial No N/A Enclosed Reference  
 Details\*
- 4) Can the system make determinations about employees/public that would not be possible without the new data?  
Yes Partial No N/A Enclosed Reference  
 Details\*
- 5) How will the new data be verified for relevance and accuracy?  
 N/A
- 6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?  
 The system contains audit, identity management, access control, role based security, network security and security zones.
- 7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.  
Yes Partial No N/A Enclosed Reference  
 Details\* The system will contain all security controls listed in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 for high impact systems.
- 8) How will the data 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.  
Yes Partial No N/A Enclosed Reference  
 Details\* This will be determine in the design phase of the project.
- 9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?  
 Auditing and or Identity Management reports are available as a part of Out-of-the-box functionality for many of the COTS tools. Reports will be utilized to provide management relevant information about user activity including but not limited to policy violations, recertification content, failed login attempts, FISMA compliancy reports, and role request changes.
- 10) Do individuals have an opportunity and/or right to decline to provide information?  
Yes Partial No N/A Enclosed Reference  
 The system may allow for users to provide or not provide content to an application for example, providing a PKI certificate to a user for acceptance into an application. If the user does not provide/share/accept this certificate information the user simply does not gain access to that application. However much of this information will need to be determined during the design phase.

- 11) Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Yes  Partial  No  N/A  Enclosed Reference

Users will be allowed consent of all or none of the user information based upon PKI certificates. If the user does not consent of this certificate information the user simply does not gain access to that application. However much of this information will need to be determined during the design phase.

**E. 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?

The system is maintained and operated in two geographical locations. Bureau of Public Debt Primary Data Center (BPD-PDC) is the primary location and FinCEN, Vienna is the disaster recovery location. The data between the two locations is kept in synchronization using Oracle Data Guard.

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

The system complies with the Department of Treasury Directive 80-50 Records and Information Management Manual. In accordance with TD 80-50, records are not destroyed or otherwise alienated from the system except in accordance with procedures prescribed in 36 CFR, Part 1228.

- 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? Records retention information for the system, its contents and any reports generated will be approved by the National Archives and Records Administration, and existing agency file plans will be revised to incorporate records information for the new system. The data will be disposed of in accordance with approved records retention instructions and procedures.

- 4) Is the system using technologies in ways that the FinCEN has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

Yes  Partial  No  N/A  Enclosed Reference

Details\* A two factor authentication method will be required for individuals accessing BSA data. The actual implementation / design of the two factor authentication will be determined.

- 5) How does the use of this technology affect public/employee privacy?

This technology secures the level of access to specific content through Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC). User privacy will also be protected with this model in a secure non-restricted / secure restricted environment.

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

Yes  Partial  No  N/A  Enclosed Reference

Details\* The identity management, access control and audit logging components of the system, will provide an audit trail of the user access to resources identified in the identity and access management systems. In addition, the user id information contained managed by the

access management user session can be leveraged by business applications to monitor users' access to finer grained application resources.

- 7) **What kinds of information are collected as a function of the monitoring of individuals?**  
The system captures all necessary data to answer the question "Who has access to What, When, and How?" This includes login attempts, access granted to the user, and connection time and duration, user identity profile history, user group membership history, user resource access and entitlement history.
- 8) **What controls will be used to prevent unauthorized monitoring?**  
Access controls are used to prevent unauthorized access to monitoring component of the system. System controls are implemented in a role- based 'least access' manner. Authorized FinCEN personnel and contractors will have the least amount of access to the system required to perform their job function. Instances of access to the system by contractors and FinCEN personnel are subject to monitoring for inappropriate activity.
- 9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**  
A new system of record notice (SORN) will be created specifically for IRIS.
- 10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**  
 Yes  Partial  No  N/A  Enclosed Reference  
 Details\* This is a new system and a SORN will be created

## F. ACCESS TO DATA

- 1) **Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, tribes, other)**  
Registered Users: The registered users are federal, state and local agencies employees and potentially members of the financial institutions.  
Coordinators: The person who provides the first level of approval after the user completes the application. Each organization or agency must have at least one Coordinator.  
Liaison Representatives: FinCEN personnel who provides the next level of approval after the agency Coordinator approves the user's application.  
FinCEN Admin: FinCEN personnel who processes user's application after the Liaison Representatives approves the application.
- 2) **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**  
  
 Access to the data by the users is determined by roles. Each user will be assigned an appropriate role (i.e., group), which are governed by the security and access policies created by FinCEN. Detail information on criteria, procedures, controls and responsibilities will be captured in the next design phase.
- 3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

Access to records in the system is limited to authorized personnel whose official duties require such access, i.e., on a "need to know" basis. Electronic data is protected through user identification, passwords, database permissions and software controls. Such security measures establish different access levels for different types of users. User's access will be restricted to their data only.

The registered user will have access to his/her own profile information.

The agency coordinator will have access to profiles of registered users from the same agency.

The FinCEN liaison will have access to profiles of the users working for the agency he/she is responsible for.

FinCEN admin will have access to all users profile information.

- 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)**  
 Security measures and controls consist of passwords, user identification, IP addresses, database permissions and software controls. All employees including contractors must meet the requirements for protecting Privacy Act protected information. The IT Security Plan describes the practice of audit trails. Audit trails maintain a record of system activity and user activity including invalid logon attempts and access to data. The C&A process require a system security plan outlining the implementation of the technical controls associated with identification and authentication. All employees, including contractors, have requirements for protecting information in Privacy Act systems
  
- 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?**  
Yes Partial No N/A Enclosed Reference  
 Details: Contractors having system access are required to have appropriate security clearances. Their contracts include non-disclosure agreements and agreements to comply with all applicable FinCEN policies and laws, including the Privacy Act.
  
- 6) **Do other systems share data or have access to the data in the system? If yes, explain.**  
Yes Partial No N/A Enclosed Reference  
 Details: The Userid will be shared across systems to maintain an audit trail of who has accessed what information. There is a potential that user contact and organization information may be unutilized by other BSA IT Mod applications.
  
- 7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**  
 All authorized FinCEN personnel, as well as authorized personnel from designated federal, state, and, local law enforcement, intelligence, and regulatory agencies that have signed a MOU with FinCEN to allow access to the BSA information will be responsible. The information owner and system manager (identified in the Privacy Act System Notice) share overall responsibility for protecting the privacy rights of individuals by developing guidelines and standards which must be followed. The external agency users will also be responsible for protecting the information. (Part of the MOU clause)
  
- 8) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**  
 Only for the purpose of background investigation conducted to verify an individual's identity.
  
- 9) **How will the data be used by the other agency?**

The agency coordinator will use the data to verify the identity of a registering user.

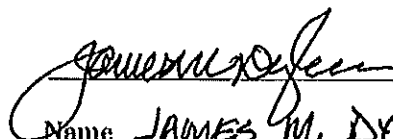
10) Who is responsible for assuring proper use of the data?

Data providers are responsible for assuring proper use of the data through various agreements and statutory mandates [i.e., the Privacy Act]. The individual applicants, as data providers, are responsible to ensure the data entered is correct.


See Attached Approval Page

The Following Officials Have Approved this Document


1) System Manager

 (Signature) 5/3/11 (Date)  
 Name JAMES M. DYKES  
 Title Senior Advisor, Infrastructure

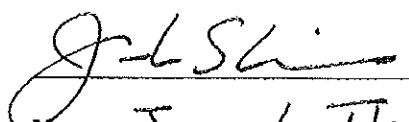
2) IT Security Manager

 (Signature) 5-3-11 (Date)  
 Name Q. Robinson  
 Title ISSO

3) Privacy Officer

 (Signature) 5-3-11 (Date)  
 Name Gayle Rucker  
 Title Privacy Admin.

4) Reviewing Official

 (Signature) 5/3/11 (Date)  
 Name Jacob Thiessen  
Privacy Act Officer

**Title**

... ..  
... ..  
... ..