



# **314(a) SISS: Secure Information Sharing System**

## **Privacy Impact Assessment (PIA)**

**314(a) SISS: Secure Information Sharing System**

Version 1.5

September 30, 2014

**Revision History**

<b>Revision Number</b>	<b>Change Effective Date</b>	<b>Description of Change</b>	<b>Change Entered By</b>
1.1	7/14/14	Updated cyber security control sections	Quentin Robinson
1.2	8/28/14	Further updates to cyber security sections.	Quentin Robinson
1.3	8/29/14	Updates agreed to in meeting of 8/27/14	Gayle Rucker
1.4	9/18/14	Updates agreed to in meeting of 9/18/14	Gayle Rucker
1.5	9/30/14	Updated from FinCEN's OGC edits	Gayle Rucker

## Table of Contents

<b>Privacy Impact Assessment (PIA) for 314(a)</b> .....	<b>3</b>
A. CONTACT INFORMATION .....	3
B. SYSTEM APPLICATION/GENERAL INFORMATION .....	4
C. DATA IN THE SYSTEM .....	5
D. ATTRIBUTES OF THE DATA .....	7
E. MAINTENANCE AND ADMINISTRATIVE CONTROLS .....	8
F. ACCESS TO DATA .....	10
<b>Approval Page</b> .....	<b>12</b>

**Privacy Impact Assessment (PIA) for  
314(a) SISS: Secure Information Sharing System**

**Name of Project:** 314(a) SISS: Secure Information Sharing System

**Bureau:** Financial Crimes Enforcement Network (FinCEN)

**Name of the system:** 314a

**Unique System Identifier:** 015-04-01-14-03-1011-00

**A. CONTACT INFORMATION**

- 1) Who is the person(s) completing this document?** (Name, title, organization and contact information).

Name: Gayle Rucker  
Organization: FinCEN  
Email: [Gayle.Rucker@fincen.gov](mailto:Gayle.Rucker@fincen.gov)

Name: Andrea Livero-Scott  
Organization: FinCEN  
Email: [Andrea.Livero-Scott@fincen.gov](mailto:Andrea.Livero-Scott@fincen.gov)

- 2) Who is the system owner?** (Name, organization and contact information).

Name: Kenneth O'Brien  
Organization: FinCEN  
Email: [kenneth.o'brien@fincen.gov](mailto:kenneth.o'brien@fincen.gov)

- 3) Who is the system manager for this system or application?** (Name, organization, and contact information).

Name: Lynda Gammon  
Organization: FinCEN  
Email: [Lynda.Gammon@fincen.gov](mailto:Lynda.Gammon@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 Privacy Act Officer (or Counsel Representative) who reviewed this document?** (Name, organization, and contact information).

Name: Albert Zarate

Organization: FinCEN  
 Email: [Albert.Zarate@fincen.gov](mailto:Albert.Zarate@fincen.gov)

- 6) Who is the Bureau Privacy Administrator who reviewed this document?** (Name, organization, and contact information).

Name: Gayle Rucker  
 Organization: FinCEN  
 Email: [Gayle.Rucker@fincen.gov](mailto:Gayle.Rucker@fincen.gov)

- 7) Has organizational privacy management information previously been provided with another PIA?**

Yes  No  N/A  Enclosed Reference

Details\* \_\_\_\_\_ Published PIA in 2008\_\_\_\_\_

- 8) If 'Yes' to Question 6, 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\* \_\_\_\_\_

- 9) Who is the Reviewing Official?**

Name: Amy Taylor, Chief Information Officer (CIO)  
 Organization: FinCEN  
 E-mail: [Amy.Taylor@fincen.gov](mailto:Amy.Taylor@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 categories of individuals covered in the system are individuals who are subjects of interest to law enforcement.

#### a. Is this information identifiable to the individual<sup>1</sup>?

---

<sup>1</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).

Yes.

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

Yes

**c. Is this information about employees?**

No.

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

The 314(a) Major Application (MA) provides financial institutions the capability to Electronically access subject lists submitted by law enforcement and to electronically report positive matches on any person or business on that subject list through a secure Internet network. 314(a) also provides a secure messaging system that allows FinCEN to communicate and disseminate information such as advisories and reports on the latest trends in money laundering or terrorist financing to the financial industry.

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

The information contained in the 314a system is collected under the authority of section 314(a) of the USA PATRIOT Act, Pub. L. 107-56 (October 26, 2001). The regulation implementing that authority appears at 31 CFR 1010.520. The authority to administer 31 CFR Chapter X, Part 1010 has been delegated to FinCEN.

**C. DATA IN THE SYSTEM**

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

The categories of individuals covered in the system are individuals who are subjects of interest to law enforcement.

**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 sources of information include federal, state, and international law enforcement agencies.

**b. Are Federal agencies providing data for use in the system?**

Yes Partial No N/A Enclosed Reference

**Details\*** The data supports sharing of information between federal law enforcement and the financial industry as covered by the Patriot Act Section 314(a).

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

Yes Partial No N/A Enclosed Reference

**Details\*** The sources of information include federal, state, and international law enforcement agencies.

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

Yes Partial No N/A Enclosed Reference

**Details\***

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

N/A

**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 are data collected from sources other than FinCEN records verified for accuracy?**

Peer review is conducted prior to the data's entry into the system.

**b. How will data be checked for completeness?**

**Peer review is conducted prior to the data's entry into the system.**

**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\*** Data older than two case postings is archived from the system.

**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\*** 314a Requirements Document

**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\***

- 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\***

The data supports sharing of information between federal law enforcement and the financial industry as covered by the Patriot Act Section 314(a).

- 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?**

**Details\***

N/A



**7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?**

Yes  Partial  No  N/A  Enclosed Reference

**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\***

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

No, the system does not create reports.

**10) Do individuals have an opportunity and/or right to decline to provide information?**

Yes  Partial  No  N/A  Enclosed Reference

**Details\***

The data gathered is for subjects of interest for law enforcement requestors as covered by the Patriot Act Section 314(a).

**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

See answer above to #10.

**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 will be maintained in all sites?**

N/A

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

**Details\***

The system complies with the Department of the Treasury Directive (TD) 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?**

**Details\***

Records retention information for the system, its contents and any reports generated will be approved by the National Archives and Records Administration (NARA) 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 FinCEN has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

Yes  Partial  No  N/A  Enclosed Reference

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

N/A; the system is not using technologies in ways that the Bureau/Office has not previously employed.

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

Yes  Partial  No  N/A  Enclosed Reference

**Details\***

This data will be used to assist in identifying and monitoring the financial activities of individuals who are potentially committing financial crimes.

- 7) **What kinds of information are collected as a function of the monitoring of individuals?**

Database auditing is done on the system. There is a comprehensive audit trail of every user and employee that logs into the system and every action taken within the system Infrastructure. IDS's and firewalls monitor any anomalies within the network. The purpose for this auditing is to ensure that only authorized users have access and make queries to the system. Persistent cookies are not used to monitor users of the system.

- 8) **What controls will be used to prevent unauthorized monitoring?**

The principle of least privilege is implemented for this system and is regularly tested by third party entities for non-compliance of security policies.

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

Pursuant to the Privacy Act of 1974, 5 U.S.C. § 552a, as amended, records filed with FinCEN under the authority set forth in section 314(a) of the USA PATRIOT Act are covered by FinCEN's Privacy Act system of records notice Treasury/FinCEN .001-FinCEN

Investigations and Examinations System. A new system of records or further alteration to our existing system of records will not be required for the 314a system.

**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\***

A new system of records or further alteration to our existing system of records will not be required for the 314a system.

**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)

**Details:** Cleared FinCEN employees, contractors, federal law enforcement partners have access to the data.

**2) How is access to the data by a user determined?** Are criteria, procedures, controls, and responsibilities regarding access documented?

**Details:** On a bi-weekly basis, FinCEN receives a point of contact listing from the federal regulators. Individuals on those listings are designated as eligible to access the system. The data can only be retrieved by a designated point of contact with a user name and password via the secure website

**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.

**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)

**Details:** No direct end-user browsing of privacy information is possible due to technical and business process limitations. Least privilege is in place for administrative technical personnel.

**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, training, 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\***

**Some PII is transferred from 314(a) to the Information Technology Infrastructure (ITI) general support system.**

**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 regulatory agencies and from financial institutions that have signed a Memorandum of Understanding (MOU) with FinCEN to allow access to the 314a information will be responsible for protecting the data. 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.

**8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**

All authorized FinCEN personnel, as well as authorized personnel from designated federal regulatory agencies and from designated financial institutions

**9) How will the data be used by the other agencies?**

This data will be used to assist in identifying and monitoring the financial activities of individuals who are potentially committing financial crimes.

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

The FinCEN Information System Owner and Information System Security Officer are responsible for the overall cyber security compliance of the system.

## Approval Page

The following Officials have approved this document –

<u>/S/</u>	<u>October 2, 2014</u>
Quentin Robinson Information System Security Officer (ISSO), FinCEN	Date

<u>/S/</u>	<u>October 2, 2014</u>
Gregory Sohn, Chief Information Security Officer (CISO), FinCEN	Date

<u>/S/</u>	<u>October 2, 2014</u>
Ken O'Brien Information System Owner (ISO), FinCEN	Date

<u>/S/</u>	<u>October 2, 2014</u>
Gayle Rucker Privacy Program Administrator (Privacy Officer), FinCEN	Date

<u>/S/</u>	<u>October 2, 2014</u>
Amy Taylor  Reviewing Official, FinCEN CIO	Date