Information Technology Infrastructure General Support System (ITI GSS) Privacy Impact Assessment (PIA)

2013 Version

September 2013

Revision History

Change Record				
Revision Number	Document ID	Description of Change	Change Effective Date	Change Entered By

Table of Contents

1. Privacy Impact Assessment Template

Name of Project: Information Technology Infrastructure (ITI)
Bureau: Financial Crimes Enforcement Network (FinCEN)
Project's Unique ID: N/A
Name of the system: Information Technology Infrastructure
Unique System Identifier: 015-00-02-00-01-1070-00

A. CONTACT INFORMATION

1) **Who is the person completing this document?** (Name, title, organization and contact information).
Name: Gayle Rucker
Organization: FinCEN
Email: Gayle.Rucker@fincen.gov

2) **Who is the system owner?** (Name, organization and contact information).
Name: Zeus Celi
Organization: FinCEN
Email: zeus.celi@fincen.gov

3) **Who is the system manager for this system or application?** (Name, organization, and contact information).
Name: Zeus Celi
Organization: FinCEN
Email: zeus.celi@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

5) **Who is the Bureau Privacy Act Officer who reviewed this document?** (Name, organization, and contact information).
Name: Jacob Thiessen
Organization: FinCEN
Email: Jacob.Thiessen@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

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

☒Yes ☐No ☐N/A ☐Enclosed Reference
Details* 2008

8) **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*
Minor Applications added:

- Agent Request Initiative (ARI) PTA was completed in February of 2012. This PTA was necessary as the collection of PII related to personal information from agents (persons) authorized to conduct business on behalf of the Money Service Business (MSB) was converted from a paper process to electronic.
- FinCEN's Separation Clearance Certification Form PTA was completed in May of 2012. This PTA was necessary because the collection of PII was converted from solely a paper process to electronic workflow and storage.
- FinCEN Reports - Electronic Suppression Requests PTA was completed in May of 2012. This PTA was necessary because a new collection method for the reports containing PII was added to the existing paper process to provide for electronic submissions.
- Currency Transaction Report ("CTR") Backfiling and Amendment PTA was completed in June of 2012. This PTA was necessary because the collection of PII was converted from a paper process to electronic.
- A new web tool designed to improve authorized users' ability to submit case requests and investigate cases, while leveraging FinCEN's BSA data analysis capabilities had a PTA completed in February of 2013.

9) **Who is the Reviewing Official?**

Ken O'Brien, Chief Technology Officer

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* This GSS and/or its supporting applications may collect the following PII:

- Employer Identification Number (EIN) or Bank Secrecy Act (BSA) Identifiers
- **Contact Information** (both personal and business) – postal mailing addresses, email addresses, phone numbers, fax numbers, etc.
- **Biometric Identifiers** - photographs, signatures, and race
- **Social Security Numbers**

- **Other Government identifiers** - national or state information, driver's license#, passport#, military id#, national ID#
- **Privacy Act Record** (SSN categorized separately) – Name, mother's maiden name, date of birth, place of birth, or national origin
- **Financial Information** - bank account information, credit card numbers, credit score, salary information, etc.
- **Other** - educational history, employment history, performance history
- **Technical and/or Location** - such as IP address, Geo-Positioning Signals (GPS) and system audit logs,

a. **Is this information identifiable to the individual?**
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?**
No, however this system's web platform supports applications whereby non-staff individuals who do business with FinCEN could submit PII. These applications' use of PII has been assessed for their privacy impact and is documented.

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

2) **What is the purpose of the system/application?**
The ITI GSS provides FinCEN it's core cyber infrastructure and contains several supporting office and business administrative applications which enable FinCEN to execute its business mission. The ITI GSS does not have a direct public facing presence. It secures applications by providing centralized authentication, authorization and auditing to enable single sign-on and secure access control

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).

C. DATA IN THE SYSTEM

1) **What categories of individuals are covered in the system?**
The system will support FinCEN internal users. ITI GSS also and provides a platform to support databases and various applications. The ITI GSS does not have a direct public facing presence but does provide infrastructure support of some web interfaces to 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 web application user will register using an online application form. The Department of Treasury's enterprise systems feed some of the PII of employees into some components of the ITI GSS, such as network user accounts. Other PII is entered directly from and by FinCEN staff.

b. **Will Federal agencies provide data for use in the system?**
☐Yes ☒Partial ☐No ☐N/A ☐Enclosed Reference
Details* The Department of Treasury's enterprise systems feed the PII of employees data into some components of the ITI GSS,

c. **Will Tribal, State and local agencies provide data for use in the system?**
☐Yes ☐Partial ☒No ☐N/A ☐Enclosed Reference
Details*

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?**
The ITI's minor applications may collect the following information from employees -
1. Employer Identification Number (EIN)

- **Contact Information** (both personal and business) – postal mailing addresses, email addresses, phone numbers, fax numbers, etc.
- **Biometric Identifiers** - photographs, signatures, and race
- **Social Security Numbers**
- **Other Government identifiers** - national or state information, driver's license#, passport#, military id#, national ID#
- **Privacy Act Record** (SSN categorized separately) - Name **and** mother's maiden name, date of birth, place of birth, or national origin
- **Financial Information** - bank account information, credit card numbers, credit score, salary information, etc.
- **Other** - educational history, employment history, etc.
- **Technical and/or Location** - such as IP address, Geo-Positioning Signals (GPS) and system audit logs, etc.

The ITI's minor applications may collect the following information from public (external web application user) –

- Tax Identification Number (TIN) or Bank Secrecy Act (BSA) Identifiers???
- **Contact Information** (business) – postal mailing addresses, email addresses, phone numbers, fax numbers, etc.
- **Biometric Identifiers** - photographs, signatures, and race
- **Social Security Numbers**
- **Other Government identifiers** - national or state information, driver's license#, passport#, military id#, national ID#
- **Privacy Act Record** (SSN categorized separately) - Name **and** mother's maiden name, date of birth, place of birth, or national origin
- **Financial Information** - bank account information, credit card numbers, credit score, salary information, etc.
- **Technical and/or Location** - such as IP address and system audit logs,

3) **Accuracy, Timeliness, and Reliability**

a. **How will data collected from sources other than FinCEN records are verified for accuracy?**
Details:
Administrative procedures ensure the accuracy of the content of the records and information input restrictions are in place in the technical systems for information accuracy, completeness, validity, and authenticity; error handling.

b. **How will data be checked for completeness?**
Administrative procedures ensure the accuracy of the content of the records and information input restrictions are in place in the technical systems for information accuracy, completeness, validity, and authenticity; error handling

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*
Administrative procedures ensure the currency of non-historical records. Document Name: <REDACTED>

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*
Privacy Threshold Analysis documents for:

- Agent Request Initiative (ARI)
- FinCEN's Separation Clearance Certification
- Electronic Suppression Requests
- Currency Transaction Report ("CTR") Backfiling
- Case Management web tool

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*
System-related information for user account management and auditing, and log information are in the ITI GSS .

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?**
Accuracy is not applicable to the ITI GSS because it is not an application. However, for the applicable Minor Child systems information input restrictions are in place for information accuracy, completeness, validity, and authenticity; error handling; and Information Output handling and retention. Administrative procedures ensure the accuracy of the content of the records and information input restrictions are in place in the technical systems for information accuracy, completeness, validity, and authenticity; error handling.

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, malicious-code protection, patch management, 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* User login name and password are part of the role-based security that controls access to the system and its data.

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
FinCEN Staff must follow existing, approved non-IT policy and procedure related to this opportunity and/or right. Business Partner POCs/ Registrants have opportunity for consent through signed form and through system/application process.

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
FinCEN Staff must follow existing, approved non-IT policy and procedure related to this opportunity and/or right. Business Partner POCs/ Registrants have opportunity for consent through signed form and through system/application process.

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. The data between the two locations is kept synchronized using technology.

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 is being deployed for user access to GSS.

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.** `Treasury/FinCEN .001 FinCEN Data Base`

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*

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 Internal Users: The registered users are federal employees and contractors
External users: The external web application user will register using an online application form
FinCEN Administrators: FinCEN staff who processes user's application and administer the ITI GSS.

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 and least privilege. 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 are contained in system and FISMA documents

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.
FinCEN administrators 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 are in place, which consist of passwords, user identification permissions and restrictive software controls. Audit trails maintain a record of system activity and user activity including invalid logon attempts and access to data. All employees, including contractors, have requirements and training for protecting sensitive personally-identifiable information (PII).

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 security and privacy policies and laws.

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 Department of Treasury systems exchange user technical administrative information.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**
All authorized FinCEN staff will be responsible. Further, those individuals listed on this document's signature page, such as the information owner and system manager (identified in the Privacy Act System Notice) as well as information system security officer, 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))?**
Some Department of Treasury systems exchange user technical administrative information.

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

Some Department of Treasury systems exchange user technical administrative information.

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

Approval Page

The following Officials have approved this document –

/S/

Quentin Robinson
Information System Security Officer (ISSO), FinCEN

10-15-13
Date

/S/

Gregory Sohn,
Chief Information Security Officer (CISO) FinCEN

10/18/13
Date

/S/

Zeus Celi,
Information System Owner (ISO), FinCEN

10/18/13
Date

/S/

Gayle Rucker
Privacy Administrator, FinCEN

10/18/13
Date

/S/

Jacob Thiessen
Privacy Act Officer, FinCEN

10/18/13
Date