DEPARTMENT OF TREASURY
Washington, D.C. 20220

Office of Foreign Asset Control (OFAC) Consolidated Technology Systems (OCTS)
Privacy Impact Assessment (PIA)

March 15, 2013

A. Identification

System Name: OFAC Consolidated Technology Systems (OCTS)
OMB Unique Identifier: 015-05-01-14-03-6002-00
System Owner: Office of Foreign Assets Control

Contact Aaron Mintz
Assistant Director, Sanctions Support Division
Office of Foreign Asset Control
Sanctions Support Division (SSD)
United States Department of the Treasury

Address: 1500 Pennsylvania Avenue, NW
Washington, DC 20220

Telephone: (202) 622-4926

B. System / Application General Information

1. Does the system contain any information in identifiable form (IIF)?

   Yes.

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

   OCTS is comprised of four (4) component applications sharing common functionality or common inherited functionally either under OFAC or Treasury Departmental Offices Control. OCTS is designated as a minor child of the Departmental Offices Local Area Network (DO LAN). OCTS provides a database service backend to support OFAC business applications. OCTS is comprised of the following OFAC component applications that reside on dedicated hardware:

- **Automated Blocking and Reject Reporting System (ABaRRS) -** ABaRRS is a customized web-based interface that electronically tracks and stores blocked or rejected transactions in accordance with U.S. economic sanctions policy.

Transaction information is either provided electronically or mailed/faxed by U.S. financial institutions. As transactions are imported into ABaRRS, they are reviewed and investigated by OFAC personnel to determine if any transaction appears to be unusual or if further action is necessary.

- **OFAC Administrative System for Investigations and Sanctions (OASIS) -** OASIS is a customized web-based repository for all OFAC correspondence and subsequent unclassified casework (in the areas of Licensing, Enforcement, Civil Penalties, FOIA, and Designation Investigations) that results. Each respective business unit has functionality to enter, review, track, assign, search and report on Case related information.

  OASIS also includes a public facing licensing component: TSRA 2.0. TSRA 2.0 is a customized web-based information system that supports OFAC's obligation to administer the sale of agricultural commodities, medicine, and medical devices to any countries supporting terrorism through one-year license agreements. TSRA 2.0 allows OFAC to store administer the license request and issuance processes. TSRA 2.0 also provides a public website that allows TSRA license applicants the ability to submit a license application over the internet.

- **Specially Designated Nationals (SDN) -** SDN is a customized web-based interface that provides OFAC personnel a standardized method for the entry of source SDN data and automates the creation and publishing of the SDN list in various formats. SDN data is unclassified and comprised of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also contains individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. All financial institutions and persons in the U.S. are required to block financial transactions that are linked to individuals, entities, and vessels that are identified in the SDN list or react appropriately to transactions that potentially violate one of the OFAC country-specific programs. The SDN List is available on the Treasury public website and a search tool is available to allow external parties and the general public the ability to search the list.

- **Service Provider Regulatory Program (SPRP) -** SPRP is a customized web-based interface that helps OFAC administer a major economic sanction program imposed by the President under authority of the International Economic Powers Act and the Trading with the Enemy Act. Specifically, SPRP provides a secure data warehouse and data entry and analysis tool for OFAC personnel to track service providers sending funds to Cuba per the U.S. Department of Treasury's trade embargo regulations. SPRP allows Treasury to track and analyze companies' financial operations and to investigate and shut down those operating illegally.

3. What legal authority authorizes the purchase or development of this application / system?

31 CFR 501.603; Reports on blocked property.

31 CFR 501.604; Reports by U.S. financial institutions on rejected funds transfers.

31 CFR 501.606; Reporting and recordkeeping requirements applicable to economic sanctions programs.

4. Under which Privacy Act System of Record Notice (SORN) does this system operate?

   DO .118 - Foreign Assets Control Licensing Records.
   DO .114 - Foreign Assets Control Enforcement Records
   DO .111 – Office of Foreign Assets Control Census Records

   http://www.treas.gov/foia/privacy/issuances/dopa.html

   A revised SORN that will apply to the OCTS is currently in final review.

C. Data in the System

1. What categories of individuals are covered in the system?

   Listed below are the systems and the types of information stored within each system.

   - **ABaRRS**: ABaRRS blocking and reject reports are generally financial transactions delivered in the form of payment instructions, letters of credit, account statements and checks. Included within this information are individual names and bank account numbers associated with blocked or rejected transactions may be present in a given blocking and reject report.

   - **OASIS**: Stores information about license application, correspondence sent to OFAC from the public or other agencies as well as documents outgoing correspondence and related license case information. The license application information and correspondence includes individual or business contract name, mailing address, telephone number, fax number, and email address.

   - **SDN**: Supports the US government's targeted economic sanctions program. Targeted economic sanctions consist of names of persons and entities that are prohibited from using the US financial system. At any given time, approximately 40 to 50 percent of the names on the list constitute the names of persons. 95 percent of these listings are non-US persons. The identifier information associated with these persons can be extensive, ranging from address and date of birth to social security numbers and passport numbers.

- **SPRP**: SPRP does not store information about individuals. SPRP stores summary information from Carrier Service Providers, Travel Service Providers, and Remittance Forwarders nationwide (collective "Service Providers") related to the services the services which the Service Providers have given to United States citizens traveling to Cuba or transferring funds to Cuba. This information covers services and accommodations necessary for Cuba travel (i.e. hotel, airline, transportation, issuance of visa, etc) or funds transfers and a summary of the dollars which the Service Providers have spent. The Service Providers, as business which provide services to United States citizens involving Cuba, submit timely and complete data to the OFAC Miami office. SPRP maintains contact information related to these Service Providers, including name, phone number, mailing address, and email address.

2. What are the sources of the information in the system?

   Information collected by OCTS is collected from external users and/or sources as well as internal OFAC staff.

   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?

      - **ABaRRS:** All ABARRS data is provided to OFAC by primarily financial institutions reporting blocked or rejected transactions per their legal obligation, however every American citizen and organization has an obligation to report blocked or rejected transactions.

      - **OASIS:** OASIS data is provided from mail correspondence, including license applications sent from the individuals or businesses/corporations to OFAC. Additionally, OASIS contains investigative research, penalty and payment information and other supplemental data that might be sent in by the public to OFAC. Case data may also be derived from the news media or Federal law enforcement agencies.

      - **SDN:** SDN data is derived from several sources, including open source/internet research, news articles, Federal intelligence data, Federal law enforcement data and data provided per international agreements and alliances with foreign governments.

      - **SPRP:** Data in SPRP is received from Miami-area travel service providers arranging travel to Cuba for United States citizens.

   b. What Federal agencies are providing data for use in the system?

      - **ABaRRS:** Federal agencies are also subject to financial transaction blocking regulations and could enter data into ABaRRS.

- **OASIS:** DHS may also provide evidence that helps resolve open OFAC cases in the OASIS system. Additionally Department of Justice, Department of State, and other Federal law enforcement agencies may also provide case data as needed.

- **SDN:** Contains information provided by various Federal law enforcement and Federal intelligence agencies related to foreign asset control.

- **SPRP:** None

c. What State and/or Local agencies are providing data for use in the system?

   There are currently no state and/or local agencies providing data to the minor applications that comprise the OCTS platform. However, State and Local governments could report blocked or rejected financial transactions through ABaRRS.

d. From what other third party sources will data be collected?

- **ABARRS:** ABaRRS data can be collected from legal entities reporting for clients or financial institutions reporting on behalf of an individual (e.g. Western Union).

- **OASIS:** None

- **SDN:** Data in the SDN system is collected from various commercial data providers, including Dun and Bradstreet.

- **SPRP:** None

e. What information will be collected from the employees, government contractors and consultants, and the public?

- **ABARRS:** Information in ABARRS may include names and account numbers along with details of blocked and rejected financial transactions collected on individuals and corporations.

- **OASIS:** OASIS captures data such as individual and business contact information, including names, address, telephone number, fax number and email address.

- **SDN:** Both the SDN system store data about designated individuals and companies. Information can include name, date of birth, SSN, document ID numbers and aliases.

- **SPRP:** SPRP stores information about service providers that are involved in travel or financial transactions between the U.S. and Cuba to include the business name, contact information and other organizational information.

3. Accuracy, Timeliness, and Reliability

   a. How will data collected from sources other than Treasury records be verified for accuracy?

      Overall, all the OCTS component applications use a three tiered architecture of information input validations to control the completeness and accuracy of the information entered. These include database constraints, business object constraints, and user interface constraints. Redundancy checks are built into the architecture so that if an input validation is missed at one tier, it can be identified at another tier. These input validation checks include reconciliations, pre-filled fields, and specific data input and pre-defined acceptable value requirements for fields. OCTS also have been developed to provide a pop up window to the end-user notifying them of the input error. When working in concert together, these information input validations have been designed to maintain data integrity within the information system and prevent erroneous information from being entered (including malicious commands).

      External OCTS users are only allowed to upload information via web-based access to ABaRRS. This information is limited to files containing blocked or rejected financial transactions. These individuals are limited to individuals with a valid user ID and password to ABaRRS Lite or an authorized Class 3 PKI certificate for ABaRRS High Volume. This input is initially processed by publicly accessible web server before being transmitted to the backend database. Before the data is transmitted to the ABaRRS backend database server, a batch process is performed to format correctly all inputted data for delivery. Once the data is correctly formatted and determined to be complete, it is transferred securely to the backend OCTS database server, OCTS internal users further process and verify the data for completeness. A two-way FTP securely transmits information between the OCTS web server and the OCTS backend database server.

      However, specific controls and processes have been built into and around each OCTS minor application to verify the completeness and accuracy of information contained within the information system. Specifically:

      - **ABARRS:** Data entry personnel compare original digital copies of payment instructions to ABARRS transaction data for completeness and accuracy.

      - **OASIS:** All licenses are received by OFAC in hard copy, manual scanned into the OASIS application, and a license case number is created. Once the license case number is created, a license officer will review the license

application information for accuracy. For any license application with inaccurate data, the license officer will either contact the license applicant for clarification or return the license to the applicant with a Return Without Action letter.

- **SDN:** Data entered into the SDN system must past a very detailed quality assurance and vetting process that requires the pending designation be vetted through a number of other federal agencies including the Department of Justice prior to publishing a revised SDN list. These checks include multiple levels of review to validate that an Unsigned Blocking Memorandum matches the original SDN data.

- **SPRP:** OFAC staff thoroughly checks and reviews all travel service provider data for completeness and accuracy and validates the information with each travel service provider.

b. How will data be checked for completeness?

See response to question 3.a. above for a discussion on completeness and accuracy controls.

c. Is the data current?

Yes, OFAC considers all data to be current at the time it is entered into the application and updated as changes occur. However OFAC is depended on the public, corporation, other Federal agencies, and third-party providers to provide changes and updates to OFAC, as necessary.

d. What steps or procedures are taken to ensure the data is current and not out-of-date?

- **ABARRS:** In accordance with legislative requirements, OFAC conducts an annual review of ABARRS data as part of OFAC's preparation of the Terrorist Asset Report (TAR). Additionally, Federal Banking and Treasury regulations require financial institutions to submit blocked and rejected transactions to OFAC as identified.

- **OASIS:** Open cases within OASIS are handled by OFAC staff who work with the applicants and other members of the public to document current and accurate information until such time that a license or case determination can be made.

- **SDN:** Information within SDN is continuously monitored and updated by OFAC throughout an investigation. Individuals and entities listed on the SDN list have the ability to petition for removal following a formal process. If such a petition is granted the name is quickly removed.

- **SPRP:** OFAC staff periodically reviews and updates travel service provider contact data in SPRP as needed through direct communication with each travel service provider.

e. Are the data elements described in detail and documented?

Yes, all data elements are documented and described 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 designed?

   Yes.

2. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? If so, how will this be maintained?

   Yes.

3. Will the new data be placed in the individual's record?

   Yes.

4. Can the system make determinations about employee/public that would not be possible without the new data?

   Yes – New data is collected throughout the lifecycle of a record to make license and investigation decisions. These determinations would not be possible without the ability to collect new/additional data about the public.

5. How will the new data be verified for relevance and accuracy?

   The new data will verified for completeness and accuracy in the same manner as discussed in the response to question 3 above.

6. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

   Not Applicable – The data within the OCTS component applications is not consolidated.

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

Not Applicable – The data within the OCTS component applications is not consolidated.

8. How will the data be retrieved? Does the personal identifier retrieve data? If yes, explain and list the identifiers that can be used to retrieve information on the individual.

   - **ABARRS:** Not applicable – Data cannot be received using a personal identifier
   - **OASIS:** A name, phone number, address, or case number can be used.
   - **SDN:** Data can be retrieved using an SSN, DOB, Name, Address and Document ID.
   - **SPRP:** Not applicable – Data cannot be received using a personal identifier.

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

   - **ABARRS:** None
   - **OASIS:** None
   - **SDN:** None
   - **SPRP:** None

E. Maintenance and Administrative Controls

1. If the system is operated in more than one site, how will the consistent use of the system and data be maintained in all sites?

   Not applicable – The system is only operated at the Main Treasury data center

2. What are the retention periods of the data in the system?

   Electronic records shall be retained online for a period of 10 years or until no longer needed for business purposes, whichever is longer. Records shall be maintained off-line for 10 years after the lifting of the applicable embargo or sanctions program.

   The exceptions to this are:

Civil Penalties case data stored in the OASIS system: Penalty payment information may be deleted 5 years after the penalty payment or debt collection.

Blocked Assets data stored in the OASIS system: Blocked Assets data is considered permanent. A complete and public access version of this data is to be sent to the National Archives at the close of the calendar year. An online agency copy is to be maintained for 10 years or until no longer needed for business purposes, whichever is longer.

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?

   OFAC document retention policies and schedules are located on the OFAC DONet Portal, and include record schedules various OFAC functional areas, including Blocked Assets, Civil Penalties, Compliance, Enforcement, Foreign Terrorists, International Programs, Licensing, Policy, Records, and Information Technology.

   The official record copy of system records whose disposition is Permanent is transferred to the National Archives and Records Administration (NARA) according to approved records schedules. Currently, a complete and public access version of data with this disposition are scheduled for annual transfer to the NARA at the close of the calendar year, with OFAC retaining a copy online ten years or until no longer needed for business purposes, whichever is longer.

   The official record copy of system records whose disposition is Temporary are retained according to approved retention schedules, and destroyed according to approved records schedules. Currently, except as noted in Item 2, data with this disposition are scheduled for retention online ten years or until no longer needed for business purposes, and are maintained offline for ten years after the applicable embargo or sanctions program is lifted at which time they may be destroyed.

4. Is the system using technologies in ways that Treasury has not previously employed (e.g., monitoring software, smart cards, caller-ID)?

   No.

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

   The technology in use within the OCTS environment is intended to assist OFAC in performing their foreign asset control obligation to the citizens of the United States, while protecting the confidentiality and integrity of the information collection on domestic citizens.

6. Will this system provide the capability to identify, locate, and monitor individuals?

   No.

7. What kinds of information are collected as a function of the monitoring of individuals?

   Not applicable – The information system is not used to monitor individuals.

8. What controls will be used to prevent unauthorized monitoring?

   Not applicable – The information system is not used to monitor individuals.

9. Under which Privacy Act SORN does the system operate?

   DO .118--Foreign Assets Control Licensing Records
   DO.114—Foreign Assets Control Enforcement Records
   DO .111 – Office of Foreign Assets Control Census Records

   http://www.treas.gov/foia/privacy/issuances/dopa.html

   A revised SORN that will apply to the OCTS is currently in final review.

10. If the system is being modified, will the Privacy Act SORN require amendment or revision?

    A revised SORN that will apply to the OCTS is currently in final review.

F. Access to Data

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

   Treasury Departmental Offices employees and contractors.

2. How is access to the data by a user determined?

   Access to each of the OCTS component applications is granted on a strict need-to-know basis and must be approved by an Information System Security Officer and OFAC Program Administrator.

3. Will users have access to all the data on the system or will the user's access be restricted?

   Each OCTS minor application uses role based security. Users are only permitted to access those items in the database to which they have been given authorized permission and based on a strict need-to-know.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?

   Entrances to the Main Treasury facility, Treasury Annex facility and OFAC offices are restricted to those employees and contractors whose work requires them to be there for the system to operate. Identification (ID) cards are verified to ensure that only authorized personnel are present. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols, which are periodically changed. Users must meet Treasury personnel security requirements defined in the Department of the Treasury Security Manual (TDP 15-71).

   User access is determined using job requirements and need-to-know. User access is enforced based on the access control concepts of least privilege and separation of duties. Access must be approved by the OCTS Information System Security Officer and an OFAC Program Administrator. User access is terminated at the conclusion of employment or a contract. Auditing features of the system are enabled to log access and attempted access. These logs are reviewed by security officers when access anomalies are identified.

5. Are contractors involved with the design and development of the system and will / are contractors involved with maintenance of the system?

   Yes.

6. Do other systems share data or have access to the data in the system? If so, explain.

   ABARRS and OASIS supply data to the OFAC Call Center System. License and Compliance case numbers and case status information is shared in an effort to aid OFAC Call Center Agents in assisting callers.

7. Who will be / is responsible for protecting the privacy rights of the public and employees affected by the interface?

   The interfaces between ABARRS and OASIS and the OFAC Call Center are internal to OFAC. Therefore, the Authorizing Official, System Owner, and Information System Security Officers of OCTS and CCS system are responsible for protecting privacy rights of this interface.

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

   The information in OCTS may be shared with Federal law enforcement officials outside of OFAC as deemed necessary and on a case by case basis. Agents and

non-agents within OFAC will have access to the information in order to resolve contact inquiries or support the mission of OFAC.

9. How will the data be used by the other agency(s)?

   The information shared with Federal law enforcement officials outside of OFAC may protect OFAC facilities and personnel.

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

    The DO Privacy Act Officer and OCTS Authorizing Official, System Owner, and Information System Security Officer all have a shared responsibility for assuring the proper use of OCTS data.