OFR OFFICE OF FINANCIAL RESEARCH

# *Office of Financial Research*
# *Constituent Relationship Management Tool*
# *Privacy Impact Assessment*
# *(“PIA”)*

***April, 2015***

## A. Identification

**System Name:** Constituent Relationship Management Tool

**OMB Unique Identifier:** N/A

**System Owner:** Mario Nardoni, OFR Associate Director, Systems Engineering

**Contact:** Andrew Krug, Associate Director, Information Security

**Address:** FOIA/PA Request
Disclosure Services
Department of the Treasury
Washington, D.C. 20220

**Telephone:** (202) 622-0930

**Fax:** (202) 622-3895

## B. System/Application General Information

**1. Does the system contain any Personally Identifiable Information (“PII”)?**

Yes.

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

The Office of Financial Research (“OFR”) manages an array of interagency, public sector, private sector, academic and other external relationships to assist with carrying out its mandates under the Dodd-Frank Wall Street Reform and Consumer Protection Act (“Act”). The Constituent Relationship Management Tool (“CRM”)  will assist OFR with: **(i)** consolidating, storing, and managing individual business contact information obtained as a result of professional relationships; **(ii)** annotating an individual’s interest and expertise in areas of financial research that align with OFR’s mission; and **(iii)** facilitating strategic or targeted outreach efforts around OFR events, announcements, and publications (including capturing interest in or attendance at past OFR events and tracking the actual number of times and circumstances in which OFR reached out to the individual).

CRM is designed to serve as an internal, centralized repository of business and professional contact information, such as names, professional affiliation, telephone numbers and other information. CRM provides a secure and efficient means of organizing and managing such information in a manner that will assist with OFR's research based mission.

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

Section 153 of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 established the purpose and duties of OFR. In order to fully and more efficiently perform the duties delineated in the Act (especially those related to supporting the work of the Financial Stability Oversight Council ("Council") and Council member agencies in the areas of data, standardization, applied and essential long-term research, and risk measurement and monitoring) OFR staff often collaborate with their colleagues in the private and public sector. The CRM assists OFR with organizing, retrieving and using contact information essential for facilitating such work.

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

The CRM system operates under Treasury .017 – Correspondence and Contact Information, and Treasury .015 – General Information Technology Access Account Records ("GITAARS").

## C. Data in the System

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

Members of the public including:

- Academia
- Business leaders and professionals in the financial industry including institutions and regulatory entities
- Members of OFR federal advisory committees, including the OFR Financial Research Advisory Committee.

**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?**

OFR receives information directly from an individual to whom the information pertains.

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

None. Federal agencies are not providing data for use in the system.

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

None. State and/or local agencies are not providing information data for use in the system.

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

None.

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

The following information will be collected:

- Full name
- Preferred name
- Organization
- Business title
- Functional title
- Line of business
- Preferred contact method
- Business address
- Business phone number
- Business email
- Business mobile phone number
- Business fax
- Assistant name, where appropriate
- Assistant title
- Assistant email
- Assistant phone
- Information regarding memberships in professional societies, affiliation with standards and bodies, any teaching positions they may have had, or any publications the individual is associated with
- Alternate contact type
- Alternate address
- Alternate phone number
- Alternate mobile phone number

- – Travel preferences (for OFR federal advisory committee members only).

## 3. Accuracy, Timeliness, and Reliability

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

Whenever OFR receives information directly from an individual, the individual providing the information will serve as verification of the accuracy, timeliness, and reliability of the information. In addition, OFR will annually review and update each CRM record by contacting the individual in a similar manner.

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

The data will be reviewed for completeness when the OFR receives it. If the data is incomplete, an OFR employee will attempt to contact the individual to ensure completeness. OFR will also review the data on a yearly basis for completeness and accuracy. If it is determined that the data is potentially incomplete, an OFR employee will attempt to contact the individual to ensure completeness.

### c. Is the data current?

Yes. Each record will contain current contact information, and is verified with the individual providing it. Individuals may also inform OFR of changes to their information. Records are also reviewed and updated during the annual record review process. In addition, if it is determined during the annual review that data is no longer current, it will be deleted.

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

OFR will receive contact information directly from the individual. OFR will annually review and update each CRM record as necessary and appropriate and may, from time to time, receive requests directly from individuals to update their records in the system. OFR may also choose to remove a contact record from use because of an inability to update out-of-date or inaccurate information. Under these circumstances the record will be changed to an “inactive” status in the system.

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

Yes. Data elements collected and maintained by the system are detailed in the following Treasury SORN: Treasury .017 – Correspondence and Contact Information.

## 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. The data is necessary to facilitate efficient communication and correspondence between OFR and its professional contacts to assist OFR in performing its research functions as delineated in the Act. It also relevant to OFR's efforts to identify opportunities for engagement or collaboration with such contacts.

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?**

   No.

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

   No new data will be created.

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

   No. No new data will be created

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

   No new data will be created.

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

   OFR utilizes a role-based access control architecture to protect data in the CRM from unauthorized access or use. Access requests receive a two-pronged review and assessment. OFR reviews the business role and responsibilities of the requestor and also reviews whether or not the requestor has a current "need-to-know" the information.

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

Processes are not being consolidated at this time.

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.**

Data is retrieved using record retrieval and search functionality within CRM. Personal identifiers can be used to retrieve data. Data can be retrieved by any of the following fields:

- Full name
- Preferred name
- Organization
- Business title
- Functional title
- Line of business
- Business address
- Business phone
- Business email
- Business mobile phone
- Business fax
- Assistant name
- Assistant title
- Assistant email
- Assistant phone
- Information regarding memberships in professional societies, affiliation with standards and bodies, teaching positions, publications an individual is associated with
- Alternate address
- Alternate phone
- Alternate mobile phone

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

The CRM permits authorized users to query the system and compile multiple records for internal OFR reporting purposes. For example, OFR will produce a report which identifies individuals who are researchers who also have an interest in a particular topic being considered for an OFR publication. OFR will also run reports to provide targeted correspondence, or to send materials to individuals interested an OFR conference or discussion topic. This capability is not used to report on specific individuals for the purpose of granting a right, benefit, or privilege, or otherwise making a determination about a single individual.

## 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?**

   The system is operated at a single site located in Washington, DC.

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

   Paper records collected in this system are retained in accordance with the National Archives and Records Administration's General Records Schedule 12, item 2a.

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 collected in this system are eligible for disposal in accordance with the National Archives and Records Administration's General Records Schedule 12, item 2a. Records will be destroyed by shredding, maceration or other similar methods. OFR will use Treasury and NARA documented records management policies, procedures, and guidelines to comply with applicable federal recordkeeping requirements for retention and disposition.

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?**

   This technology does not significantly impact public or employee privacy because it does not use technologies in ways that Treasury has not previously employed. The information is collected directly from the individual and used for the limited purpose of identifying and contacting experts in areas relevant to OFR's mission.

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

   The system is not designed for the long term tracking of individuals. Individuals may be identified and located through their contact information contained in the system, but the system is not configured to monitor nor will it be used to monitor individuals.

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

None.

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

User access is restricted to the data required for the performance of their duties. Users also receive (and must acknowledge) OFR Rules of Behavior for the appropriate use of OFR information technology and resources and must complete annual privacy and security awareness training. Additionally, users logging into CRM are prompted with a warning banner noting acceptable system use and security requirements. Finally, system use is audited in accordance with OFR IT security policies and procedures as described in Section F4 below.

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

The CRM operates under Treasury .017 – Correspondence and Contact Information, and Treasury .015 – GITAARS.

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

The system is not being modified.

## F. Access to Data

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

OFR users, system managers, and system administrators, as well as contractors and their sub-contractors acting on behalf of OFR with a need-to-know the data contained in the system in order to perform their duties.

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

Users are granted access based on: **(i)** a demonstrated need-to-know in support of their job responsibilities; and **(ii)** managerial decisions.

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

Users are restricted to the accessing only the data needed in the performance of their duties. Depending on their role in administering, supporting, and maintaining the system, some users will be granted access to all of the data while other users will be granted restricted access to the data.

System access and permissions vary. The CRM user roles and responsibilities include the following:

- **Associate Director:** CRM owner, add/update records, run reports and extracts, change record status, able to view all records and fields.

- **IAR Team:** CRM record owners, add/update records, run reports and extracts, change record status, able to view all owned records and fields, able to view all other records with selective access to restricted fields, able to create workflows, fields, and entities and configure screens.

- **Front Office:** Add/update records, able to view all records with selective access to restricted fields.

- **Research & Data Services**: Add/update records, able to view most records. Unable to view restricted fields.

- **External Affairs**: Add/update records, able to view most records

- **Administration:** Add/update records, able to view most records

- **Technology:** Add/update records, able to view most records, able to create workflows, fields, entities and configure screens.

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

   User access is restricted to the data required for the performance of their duties. Users also receive (and must acknowledge) OFR Rules of Behavior for the appropriate use of OFR information technology and resources and must complete annual privacy and security awareness training. Additionally, users logging into CRM are prompted with a warning banner noting acceptable system use and security requirements. Moreover, OFR has also implemented controls to prevent the misuse of information contained in the CRM system. Finally system access and use is audited and monitored in accordance with OFR IT security policies and procedures.

   Moreover, event logs and log management systems are secure and access is limited to only authorized staff. Audit logs and audit settings are prohibited from being tampered with, deleted, or disrupted. Any changes must be approved through a formal change request.

   Additionally, users are prompted with a warning banner upon logging into CRM noting acceptable use and security requirements of the system.

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.**

   No.

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

   There is no public interface. However system users, the system security manager, system owner, and the OFR Chief Counsel's office share responsibility for protecting the privacy rights of individuals whose information is maintained in the system.

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

   No.

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

   N/A

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

    Employees who have access to the system, the system security manager, system owner, and the Chief Counsel's office are responsible for assuring the proper use of the data in the system.

## THE FOLLOWING OFFICIALS HAVE APPROVED THIS DOCUMENT

1. **Authorizing Official**

John Talbot Digitally signed by John Talbot [redacted] Date: 2015.04.17 16:16:02 -04'00'

________________________________ **(Signature)** **Date** ____________

**Name:** John Talbot **Title:** OFR Chief Technology Officer

2. **System Owner**

Mario A Nardoni Digitally signed by Mario Nardoni [redacted] Date: 201 .04.17 14:07:21 04'00'

________________________________ **(Signature)** **Date** ____________

**Name:** Mario Nardoni **Title:** OFR Associate Director, Systems Engineering

3. **Information Systems Security Manager (ISSM)**

Andrew Krug Digitally signed by Andrew Krug [redacted] Date: 2015.04.17 15:43:34 -04'00'

________________________________ **(Signature)** **Date** ____________

**Name:** Andrew Krug **Title:** OFR Associate Director, Information Security

4. **Deputy Assistant Secretary for Privacy, Transparency, and Records**

Helen G Foster Digitally signed by Helen g. Foster Date: 2015.04.20 12:40:20 -04 00

________________________________ **(Signature)** **Date** ____________

**Name:** Helen Goff Foster **Title:** Deputy Assistant Secretary
Privacy, Transparency, and Records
Department of the Treasury