

PRIVACY IMPACT ASSESSMENT

Contractor Management System (CMS)

May 2012

FDIC Internal System

Table of Contents

[System Overview](#)

[Personally Identifiable Information \(PII\) in CMS](#)

[Purpose & Use of Information in CMS](#)

[Sources of Information in CMS](#)

[Notice & Consent](#)

[Access to Data in CMS](#)

[Data Sharing](#)

[Data Accuracy in CMS](#)

[Data Security for CMS](#)

[System of Records Notice \(SORN\)](#)

[Contact Us](#)

System Overview

The Federal Deposit Insurance Corporation (FDIC) is an independent agency of the U.S. government charged with maintaining stability and public confidence in the nation's financial system. Within FDIC, the Division of Resolutions and Receiverships (DRR) promotes confidence in the nation's financial system by paying insured depositors quickly and effectively managing failed banks. DRR currently utilizes both employees and contractor staff to achieve its mission and ensure DRR's continued readiness to handle all aspects of bank closings.

To this end, the Contractor Management System (CMS) allows DRR's Contract Oversight Section to track and monitor contractors supporting financial institution/bank closing activities managed by DRR, as well as contractors providing operational support to the DRR Contract Oversight Section. CMS provides a secured environment for managing the employment status, clearance status, assignments, and departure dates of these DRR contractors. CMS is also used to track FDIC information technology (IT) devices and hardware, such as tokens and computers that are issued to DRR contractors. The data maintained in the system is collected from forms or from available information reviewed and provided by management.

The primary business function supported by CMS is to assist DRR with the management of relationships between contracts, task orders and the contractors assigned to these task orders. However, data in CMS also may be used by DRR Contract Oversight staff to respond to DRR Investigations' inquiries regarding Persons of Interest (POI)¹. In this case, DRR Contract Oversight staff check CMS on behalf of DRR Investigations and verify the individual contractor's full name and last four digits of SSN. This use of CMS is necessary to reduce the risk to the Corporation of employing or retaining individuals who are suspected of involvement in the failure of a financial institution.

Personally Identifiable Information (PII) in CMS

CMS contains both personally identifiable information (PII) and non-PII about prospective, current, and former DRR contractors who support, supported, or may support on-site and off-site bank closing activities managed by DRR, as well as DRR contractors providing operational support to DRR's Contract Oversight Section. The following data elements relating to these individuals are maintained in CMS:

- Full Name
- Company Name
- Date of Birth (DOB)
- Social Security Number (Only the last 4 Digits of the SSN are contained in the system)
- Employee Identification Number (CMS-generated identifier)

¹ Persons of Interest (POI) refers to individuals who are suspected of involvement in the failure of financial institutions, such as directors, officers, fidelity bond companies, attorneys, accountants and other parties. When the FDIC is appointed Receiver of a failed institution, the primary objective of DRR Investigations staff is to identify fraud at the failed institution and maximize recoveries for the Receivership. DRR Investigations staff work closely with attorneys in the FDIC Legal Division, Professional Liability Group (PLG) Section, to uncover and develop professional liability claims which may be brought against PIs. As part of this process, POI data is collected by DRR Investigations staff and may be used to screen potential FDIC job applicants and contractor personnel to ensure they meet FDIC's Integrity and Fitness standards.

- Contractor Status with regards to FDIC Work Assignments (i.e., Assigned, Unassigned, Expired)
- Prior Financial Institution Experience: This information is used for determining the types of skill sets a contractor may have that can be suitable for certain assignments. It includes whether or not the contractor has prior work experience at a financial institution and, if so, the institution name*, role performed*, and start and end dates*.
- Work Telephone, Work Email Address*, and Network ID*
- Tracking Dates, including Date Confidentiality Agreement Recorded* and Background Investigation (BI) Status Dates (i.e., Submission of BI Package Date, Letter of Inquiry (LOI) Issue Date*, Clearance Date)
- Clearance Status (i.e., Pending, Granted, Rejected, Expired)
- Assets (i.e., FDIC-issued IT devices and hardware) assigned to the contractor
- Attachments, such as signed FDIC Confidentiality Agreements which include contractors' names and signatures.

*Completion of these data fields in CMS is optional.

Purpose & Use of Information in CMS

The use of data in CMS is relevant and necessary to the purpose for which the system was designed, namely to support the management and tracking of DRR contracts, task orders, and individual contractors assigned to assist with various DRR job tasks including bank closings. The use of personal data about contractors in CMS is also necessary to verify POI requests from DRR Investigations.

Sources of Information in CMS

Sources for the information collected and maintained in CMS include:

- **Division of Insurance and Research (DIR) Structure Information Management System (SIMS):** SIMS maintains non-financial data (or "structure data"²) for all institutions insured, supervised, and monitored by FDIC. Via an automated system "service call," current SIMS data about financial institutions (non-PII) can be used to update contractors' work assignment records in CMS. This SIMS data includes the following non-PII about financial institutions: Certificate Number, Financial Institution Number (FIN) (if applicable), Institution Name, City and State. CMS does not share SIMS data with any other application and SIMS does not retrieve or receive any data from CMS.
- **Contracts track Orders:** The contract type, number, scope, and contact information for a POC at the contract company are derived from the contract that is executed by FDIC's Acquisition Services Branch (ASB) within the Division of Administration (DOA). The Contract Oversight Section enters this contract data into CMS, along with non-PII about FDIC task orders (e.g., task

² Structure data, which is public in nature, encompasses attribute, classification and ownership information for financial institutions.

- order number, type, category, start/end dates, etc.) which is obtained from the FDIC-issued task order.
- **Background Investigation (BI) Forms:** The contractor name, DOB, Last 4 digits of SSN, prior financial institution employment history, and assignment data is collected from the background investigation (BI) forms completed by the individual contractor and submitted to the Oversight Manager (OM) or OM designee for review and quality control. The aforementioned data is entered directly into CMS by the OM or another authorized member of the Contract Oversight Section.
 - **Background Investigation Correspondence:** The contractor's clearance status and BI status dates (i.e., submission date of BI forms, issue date of Letter of Inquiry, and clearance date) are derived from correspondence with FDIC Division of Administration (DOA) Security & Emergency Preparedness Section (SEPS). Specifically, the Contract Oversight Section forwards the contractor's completed BI documents to SEPS and then updates CMS with the date the BI forms were submitted. SEPS performs a preliminary BI check in order to determine whether the individual is suitable for employment. If SEPS identifies potential BI issues, SEPS notifies the Contract Oversight Section and issues a Letter of Inquiry (LOI) to obtain more information from the contractor. Based on this notification from SEPS, the Contract Oversight Section updates the LOI issue date field in CMS. Once SEPS makes a preliminary suitability determination, SEPS sends an email to the Contract Oversight Section indicating whether or not the individual contractor is cleared to work. This email is used by the Contract Oversight Section to update the contractor's clearance status and, if applicable, clearance date in CMS.
 - **Attachments:** Attachments related to individual contractors, contracts and task orders can be uploaded into CMS by the Contract Oversight Section. Examples of such attachments include: contractors' signed FDIC Confidentiality Agreements, copies of the actual task orders, and the contract management plan. These attachments generally contain minimal or no PII.

Notice & Consent

Individuals do not have the option to "opt out" from providing personal information. The personal information in CMS about individual contractors is obtained primarily from background investigation (BI) documents sent to the Oversight Manager or other authorized Contract Oversight Section employees. The contractor information that is entered into CMS is necessary for managing the status of DRR contractors, their clearance status, bank closing assignments, FDIC-assigned assets/hardware, and departure dates. In addition, the contractor's full name and last four digits of SSN are necessary for verifying POI requests from DRR Investigations.

Access to Data in CMS

The primary users of CMS include authorized DRR Contract Oversight Section employees in support of their oversight of DRR contractors assigned to work on the resolution of failed financial institutions. In this capacity, authorized users in the DRR Contract Oversight Section require access to CMS in order to analyze and track contractor on-boarding and departure status; maintain data about contracts and task orders; assign contractors to task orders; maintain relationships between contractors and the task orders; and, as needed, verify DRR Investigations' POI requests. In addition, authorized DRR Contract Oversight personnel also require access to CMS to track FDIC IT devices and hardware, such as tokens and computers, issued to DRR contractors.

Other authorized FDIC users are within the Division of Information Technology (DIT), which is responsible for providing technical support during the construction of the system; confirming adherence to FDIC security and privacy policies and standards; and providing system administration and maintenance support upon completion.

Data Sharing

Other Systems that Share or Have Access to Data in the System:

System Name	System Description	Type of Information Processed
N/A	N/A	N/A

Data Accuracy in CMS

Data entry screens include edit checks to ensure that business rules and data relationships are maintained. Data validation has been incorporated within the application (front-end) and the database (back-end) to ensure data is entered in the required format. There are validations at the data field level (e.g., monetary fields must be numeric). There are calculated fields to avoid manual entry errors.

Data Security for CMS

All authorized users requiring access to CMS data must have the prior approval of their Manager/Supervisor and the DRR CMS Program Manager/Data Owner. Additionally, CMS's functional security limits a user's access to specific role-based functions and regulates a user's ability to update data for a specific function. Access to the system is determined on a "need-to-know" basis and dependent on the specific user's job requirements; managerial decisions; and the purpose for which the data was collected. The criteria, procedures, controls and responsibilities regarding access comply with the Corporation's Access Control Policies and Procedures. Controls are documented in the system documentation, and users' access is tracked in the Corporation's access control tracking system.

An audit trail process captures data manipulations (i.e., Insert, Update or Delete), identifying who performed the data manipulation and when the data manipulation was performed. Corporate Information Security Awareness training and Privacy Act Orientation, which includes Rules of Behavior, are mandated for all users of the CMS system. This training has specific information regarding compromise and the prevention of misuse of data. All employees and contractors must take the training on an annual basis and certify that they agree to abide by the Rules of Behavior to retain access to the system.

System of Records Notice (SORN)

CMS operates under the FDIC Privacy Act SORN, 30-64-0015, *Personnel Records*.

Contact Us

To learn more about the FDIC's Privacy Program, please visit:

<http://www.fdic.gov/about/privacy/>.

If you have a privacy-related question or request, email Privacy@fdic.gov or one of the [FDIC Privacy Program Contacts](#). You may also mail your privacy question or request to the FDIC Privacy Program at the following address: 3501 Fairfax Drive, Arlington, VA 22226.

