PRIVACY IMPACT ASSESSMENT

INTRODUCTION

The objective of the Privacy Impact Analysis (PIA) is to determine the scope, justification, and Privacy Act applicability for systems collecting, storing or processing sensitive, personal data that may be considered private. Upon completion of the questionnaire and acquisition of signatures, please return to DIT Information Security Staff located in Virginia Square, Room Number A7032.

Agency: **Federal Deposit Insurance Corporation (FDIC)**

System Name: **Control Totals Module**

System Acronym: **CTM**

System Owner/Division or Office: **Division of Receiverships and Resolutions (DRR)**

A. Information and Privacy

To fulfill the commitment of the FDIC to protect personal data, the following requirements must be met:

- Use of the information must be controlled.
- Information may be used only for necessary and lawful purposes.
- Information collected for a particular purpose must not be used for another purpose without the data subject's consent unless such other uses are specifically authorized or mandated by law.
- Information collected must be sufficiently accurate, relevant, timely, and complete to ensure the individual's privacy rights.

Given the vast amounts of stored information and the expanded capabilities of information systems to process the information, it is foreseeable that there will be increased requests, from both inside and outside the FDIC, to share sensitive personal information.

C. System Description

This section of the Privacy Impact Assessment (PIA) describes the application and the method used to collect, process, and store information. Additionally, it includes information about the business functions the system supports.

The Federal Deposit Insurance Corporation (FDIC) is an independent agency of the U.S. government that protects the funds depositors place in banks and savings associations.

In the event of a bank failure, the FDIC, in its Receivership capacity, assumes the task of settling the debts and selling/collecting the assets (i.e., loans) of the failed institution and its Subsidiaries.[1] The FDIC either sells the loans at the time of the bank's closing or retains the loans temporarily.

Within FDIC, the Division of Resolutions and Receiverships (DRR) has primary responsibility for handling the resolution of failed banks. One of DRR's key responsibilities is completing the financial accounting process known as Proforma, which is the process of bringing the failed institution's accounting records, or General Ledger (GL), into balance as of the closing date. DRR Accounting staff then enters journal entries about the Proforma results into DRR's Control Totals Module (CTM) system, which is used to to help track and process financial accounting information pertaining to Receiverships and their Subsidiaries.[2]

With the exception of disbursement processing,[3] CTM serves as the primary financial processing, research and reporting system for Receiverships and their Subsidiaries. Specifically, CTM is used by DRR Accounting and other staff to support the following primary business functions:

- Recording Receivership and Subsidiary cash receipts (i.e., incoming monetary items, such as cash, checks, wires, etc.);
- Processing financial transactions;

[1] Subsidiaries refers to Joint Ventures, Limited Liability Companies (LLCs), Corporations, trusts or partnerships that are owned in full or part by the failed institution. The types and lines of business for these Subsidiaries vary (e.g., credit card operations, mortgage companies, travel agencies, real estate holding companies, loan servicing, equipment leasing, real estate development, consumer finance, and insurance companies, etc.). Since the Subsidiary is a separate legal entity, the failure of the bank does not cause the Subsidiary to also fail. The FDIC, as Receiver, elects Subsidiary Directors who in turn appoint Subsidiary Officers to manage the operations and assets of the Subsidiary until it is sold or liquidated, and the Subsidiary is dissolved.

[2] When an Assuming Institution (AI) acquires the failed institution, Proforma also entails creating two sets of accounting books: one for the AI and one for the Receivership. The final balance sheet is used to divide the failed bank's assets and liabilities between the receivership and assuming institution. To learn more about the FDIC bank closing process, visit http://www.fdic.gov/bank/historical/reshandbook/.

[3] Disbursement processing refers to processing accounts payables, payment of dividends, or writing checks. CTM is not used to handle such disbursement processing.

- Maintaining the Subsidiary Ledger[4] for selected General Ledger accounts; and
- Maintaining, tracking and reconciling the balances of serviced assets (e.g., loans) and other selected General Ledger accounts.

Each of the CTM system sub-modules (also known as facilities) that support the functions listed above have internal edits and controls appropriate to ensure accounting integrity for a system that generates financial accounting activity that is posted to the FDIC's General Ledger.

While CTM primarily includes financial accounting data, certain modules may contain limited Personally Identifiable Information (PII) about individuals who had a financial relationship with the failed bank or the FDIC, in its Receivership capacity. For more information on the types and uses of PII contained in CTM, please refer to Section D of this Privacy Impact Assessment (PIA).

D. Data in the System

1. What personal information about individuals or other information that can personally identify an individual (name, social security number, date of birth, address, etc.) is contained in the system? Explain.

   CTM may include limited Personally Identifiable Information (PII) as described below:

   Payor Information: The Cash Receipts module in CTM may include information about entities and individuals who make payment to FDIC in the form of a check or some other mechanism. While payor information in CTM typically pertains to businesses or entities, in certain instances, the payor information could pertain to an individual. For example, CTM may contain PII about borrowers of failed institutions who remit mortgage loan payments directly to the FDIC or through third party, interim or external asset servicers. The specific data elements that may potentially be contained in CTM about payors include:

   - **Payor Name**: This refers to the name of an entity or individual who remitted payment to the Receivership/Subsidiary for a mortgage loan or other service/obligation.

[4] Businesses often use several different ledgers and journals to maintain records of financial transactions. A Subsidiary Ledger is a special or supporting ledger that provides more detailed information about individual accounts than the General Ledger. The total of all individual accounts in a Subsidiary ledger equals the balance of the corresponding summary account (or control account) in the general ledger. CTM is responsible for acting as the Subsidiary ledger for selected General Ledger account numbers. The accounts tracked by CTM currently include collection related liabilities, miscellaneous accounts receivable and various other asset and liability accounts.

- **American Bankers Association (ABA) Routing Number**: This refers to the ABA number associated with the entity or individual's checking account from which a deposit was made.
- **Source Account Number**: This refers to the individual or entity's bank account number that was the source of the deposit.
- **Check/Wire Number, Payment Amount, & Date Received**: This refers to the check number or the wire confirmation number associated with a cash receipt, the amount remitted by the payor, and the date the cash receipt was received by the FDIC.

Customer Information: Customers may be business entities or individuals that are associated with miscellaneous accounts receivable/payable items in CTM. Generally, customers are businesses/vendors that have a financial relationship with Receiverships or Subsidiaries (i.e., owe money to, or are owed money by, the Receivership). In limited circumstances, a customer may be an individual, in instances where a small business/vendor uses his/her own name as the name of his/her business. CTM may contain the following information about each customer: customer name and the associated amount of money that the customer paid to, or is to-be-paid by, the FDIC. Also, while DRR receives customer contact information (address, phone, contact name) from servicers, this data is not used by or stored in CTM, but in a separate DRR system, 4C.[5] In extremely rare instances, a customer's address and telephone number may be manually entered into CTM for certain non-serviced assets, such as miscellaneous accounts receivables/payable items.

Property Information: A property address associated with certain miscellaneous accounts payable/receivable items may be included in the "Remarks" field in CTM. However, the property address is typically not associated with or linked to an individual person.

Participant Information: CTM may include information about participants, which are entities with an ownership interest in serviced assets. Since banks typically do not deal with individuals when structuring participation[6] agreements, the participant information in CTM

[5] For further information about DRR's 4C system, see the Privacy Impact Assessment at www.fdic.gov.

[6] There are two categories of participations: (**1) Participation Purchased –** A participation purchased is the portion of a loan purchased from another financial institution or agency. The failed financial institution owns a portion of the loan and the servicing of the loan is done by an entity other than the failed financial institution. The loan may or may not be carried on the Subsidiary System of Record, but will be recorded on the General Ledger. The financial institution usually does not receive payments directly from the debtor, but rather from another institution or agency. **(2) Participation Sold –** A participation sold is a loan which was originated by the failed financial institution, which then sold an equity interest in the loan to a third party(s). The gross amount of the loan (whole loan) is usually recorded on the failed financial institution's books with a contra asset(s) reflecting the amount sold to the participant. However, some institutions may carry these assets on a net basis. DRR Accounting personnel must determine how the financial institution identified and accounted for participations sold on the Subsidiary system of record and the General Ledger.

generally always pertains to business entities and financial institutions (e.g., Small Business Administration, other banks, etc.), not to individuals. CTM includes the participant name, amount, and non-PII identifiers associated with the participant, including the 4C Asset ID number and Servicer ID.

Trustee for Owner (TFO) Information: The TFO module in CTM is used to track and manage the account balances for funds that are received and held by FDIC on behalf of third parties, until they are disbursed or otherwise processed in a future transaction. These funds are classified by product code/type of fund, such as earnest money deposits, pensions, lost pensions, taxes, and miscellaneous fund types. While the TFO module generally contains non-PII (such as fund number, product code, and current balance), the "Description" field may contain the name of the business entity or individual(s) from whom payment was received for pertinent funds and, in very limited circumstances, the address of the Owned Real Estate (ORE) property that these entities or individual(s) purchased, if applicable. Generally, though, the TFO module only contains information pertaining to businesses, not to individuals.

DRR CTM System User Information: CTM contains a User Name and User Email Address for each system user. Note: CTM previously contained Social Security Numbers (SSNs) from DRR CTM system users and Tax Identification Numbers (TINs) from Customers and Servicers. This is no longer the case. SSNs and TINs have been removed or replaced with generic numbers.

2. Can individuals "opt-out" by declining to provide personal information or by consenting only to a particular use (e.g., allowing basic use of their personal information, but not sharing with other government agencies)?

   ☐ Yes Explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data):

   ☒ No Explain: Personal information contained in CTM is not obtained directly from individuals, but instead through transfers of data directly to DRR from the failed institution via DRR's Business Information System (BIS) staff, interim servicers, external asset servicers, asset service providers, and other third-party sources as described in Section D.3 of this PIA. This information is necessary to support FDIC's critical Receivership functions pertaining to processing, tracking, and reconciling financial transactions and balances for Receiverships and their Subsidiaries. Therefore, there is no opt-out option for these individuals.

3. What are the sources of the information in the system? How are they derived? Explain.

Non-PII Sources[7]

Failed Bank/Institutions: At the time of the bank's closing, the DRR Accounting staff manually enters journal entries about the Proforma[8] results into CTM. No personal information is contained in these journal entries.

Failed Bank Interim Servicers: DRR BIS sets up a Secure File Transfer Protocol (SFTP) website to obtain data from a variety of interim servicers[9] and then loads the data to 4C. Via a batch process, CTM periodically reaches out to a 4C network folder and transfers in these Interim Servicing files for processing. The files contain asset IDs (numeric identifiers that are assigned/used by the servicer) and asset balances (gross balances, participated sold balances, net balances, etc.). No personal information is loaded to CTM as part of this process.

FDIC 4C System: 4C provides several files of data to CTM, none of which contain PII. As background, these files include: a file with data participant information (name of participant entity (not an individual), relationship to servicer, and asset number); a file with interim servicing data (asset number and balance); a file with asset number and balance for assets that are being moved out of interim servicing and converted to Type 45 Assets ("Other Assets") in CTM; and a file that contains the asset names for Type 45 Assets/Other Assets. Since Type 45 Assets do not pertain to individuals, the "Asset Name" field in this file does not contain the name of a borrower or individual.

FDIC New Financial Environment (NFE) System: NFE is the Corporation's main financial management and accounting system. CTM interfaces with NFE to validate "product codes" tied to the type of asset

[7] Non-PII Sources refers to FDIC and non-FDIC sources that provide information to CTM, but do not provide PII for use in the system.

[8] Proforma is the confirmation of the bank's final balance sheet. The Proforma adjustment process includes any adjustments necessary to reconcile the general ledger balances to its sub systems (loans, deposits etc.) and to reflect the purchase of assets and the assumptions of liabilities by the assuming bank.

[9] For approximately 90 days following a bank closing, FDIC may use the servicer of the failed institution on an interim basis, as DRR works to sell any assets not initially transferred to an acquirer. Assets remaining after this period are converted from interim servicers to asset service providers or external asset servicers who work to sell the assets on behalf of the Receivership.

being accounted for in CTM. NFE also provides CTM with updated General Ledger balances, which are used to compare to the balances in CTM. No personal information is provided to CTM by NFE.

PII Sources[10]

FDIC Contract Asset Servicers (External Asset Servicers): External asset servicers[11] refers to third-party firms that are under contract to service assets on behalf of FDIC. These firms provide files with data on serviced asset transactions and balances to DRR via secure FDIC-furnished transfer mechanisms (e.g., SFTP). The files provided by external asset servicers primarily contain financial data, not PII, and are used to update Subsidiary Systems of Record (SSR)[12] balances and create journal entries in CTM. In certain instances, a file could potentially contain borrower name in the "Asset Name" field, but this is not common. The files are loaded into a backend database table within CTM that is archived and is not available to any CTM system users. Only financial information, such as the 4C identifier, outstanding balance, participating balance, and financial transaction details, from these files is made available to authorized CTM system users. None of the potential PII (i.e., borrower names) contained in these files is available to or searchable by CTM system users.

Application Service Provider (ASP): ASP[13] refers to a loan servicing platform that the FDIC, as Receiver, uses to track assets[14] that are not maintained by external servicers. Assets are added to the ASP system and then all payments, adjustments, or advances are applied in-house by FDIC personnel. ASP periodically provides CTM with data files of asset transactions and balances that are used to update SSR balances for each asset and to create journal entries that record the financial transactions. This data generally contains the ASP servicer ID and asset name (which

[10] PII Sources refers to FDIC and non-FDIC sources (e.g., loan servicers, banks) that provide information to CTM, including but not limited to PII for use in the system.

[11] The FDIC is currently contracting with the following external asset servicers: Ocwen, Nationstar, KeyBank, Midland, and NewTek.

[12] Subsidiary System of Record (SSR) balances represent the balance for the grouping of accounting information as it is reflected in the actual system of record.

[13] The current ASP system utilized by FDIC is Metavante. Metavante resides off-site from the FDIC and is owned, operated, monitored, and maintained by FIS, a third-party vendor. Assets are added to the Metavante system and then all payments, adjustments, or advances are applied by FDIC personnel. Metavante interfaces to CTM for processing to the FDIC's General Ledger.

[14] These assets consist mainly of assets taken at bank closings. Specifically, the assets maintained in Metavante-Insight are loans, owned real estate, securities, and off book assets (i.e., restitution orders, liability claims, etc.) of failed financial institutions. Cash payments and other reductions are applied to the assets through Metavante-Insight.

may contain PII, such as borrower name, in limited instances as described above). However, of the information provided by the ASP, only financial data (no personal information) is made available to system users in CTM

FDIC's Wire Deposits Banks: Wire deposit banks provide DRR with a file of cash receipts deposited into the FDIC account maintained for Receiverships and their Subsidiaries.[15] This file may contain PII, such as payor name (which potentially may be an individual or borrower who remitted money to the Receiver), bank account number, and ABA routing number. Authorized CTM users upload the file to CTM; the file creates cash receipt records in the Corporation's General Ledger.

FDIC's Lockbox Bank: The FDIC's Lockbox Bank, currently JP Morgan Chase (JPMC), provides DRR with a file of cash receipts deposited into the lockbox for Receivership and Subsidiary bank accounts. This file may contain PII, such as payor name (which potentially may be a borrower who remitted money to the Receiver), bank account number, and ABA routing numbers. The file is uploaded to CTM by authorized users and creates cash receipt records.

DRR CTM System Users: Data is created in the system through online data entry by authorized DRR CTM system users. For example, at the time of the bank's closing, the DRR Accounting staff manually enters journal entries about the Proforma results into CTM. No personal information is contained in these journal entries. Another example of manual entry is when authorized DRR Accounting staff manually record information about miscellaneous accounts receivables/payable items and cash receipts (payor name, amount remitted, account number, ABA number, and check number, if applicable) in CTM.

4. What Federal agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

   No Federal agencies provide data for use in the CTM system.

5. What state and local agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

   No state and local agencies provide data for use in the CTM system.

[15] DRR currently uses the Federal Home Loan Bank and Chase Bank to process wire deposits.

6. What other third party sources will be providing data to the system? Explain the data that will be provided, the purpose for it, and how will it be used.

   Please refer to Section D.3 of this PIA for a list of the third-party sources that provide data to CTM, as well as an explanation of the purpose and use of the data they provide.

E. Access to Data:

1. Who will have access to the data in the system (e.g., users, managers, system administrators, developers, contractors, other)? Explain their purpose for having access to this information.

   Users of the system include: authorized FDIC DRR Accounting and other staff, supervisory personnel, management officials, system administrators and other employees of the Corporation who have a "need to know" the information contained in this system in order to carry out their duties. In certain circumstances, a limited number of Division of Finance (DOF) staff may have access to CTM in order to perform their respective financial/ accounting business functions. In certain instances, contractors performing work on the Corporation's behalf may have access to records in the system.

   In addition, FDIC Division of Technology (DIT) and DRR information technology employees and contractors may have access, as necessary, to administer and support CTM operations. Developers have access to the data in the non-production environments. They use this data to test application corrections and changes. Developers have access to the data in the production environment through the use of an On Call ID. Access to this ID is tracked and reviewed and its use is justified each time it is activated. This access is used to research and resolve production processing problems.

   All contracted users must sign a Contractor Confidentiality Agreement.

2. How is access to the data determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Explain the process.

   All authorized users who have access to the CTM data must have the approval of their Manager/Supervisor and the DRR CTM Program Manager/Data Owner before access is granted to the system. Additionally, CTM's functional security limits a user's access to specific

functions and regulates a user's ability to update data for a specific function.

All access granted is determined on a "need to know" basis. Guidelines established in the Corporation's Access Control Policies and Procedures document are also followed. Controls are documented in the system documentation and a user's access is tracked in the Corporation's access control tracking system.

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

   Access to 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 and software controls. Such security measures establish different access levels for different types of users.

   User access to data is limited based on the assigned processing location. Users associated with one processing location cannot view or update data associated with other processing locations. Currently, the FDIC only has one active processing location.

4. What controls are in place to prevent the misuse (e.g., browsing) of data by those having access? (Please list processes and training materials) Explain the controls that have been established and how are they monitored or reviewed.

   An audit trail process captures activities performed on datasets and alerts CTM security staff with the daily report for review for unauthorized/ suspicious activities. In addition, CTM users are required to take the FDIC's Information Security & Privacy Act Orientation training which includes the Rules of Behavior. This training has specific information regarding compromise and the prevention of misuse of data.

5. Do other systems share data or have access to the data in the system? If yes, explain the purpose for the need to have access.

   Yes, data from CTM is provided to the following FDIC systems:

   FDIC NFE System: CTM passes a flat file of financial transactions and asset servicer information (business names and ID numbers of active asset servicers) to NFE. No PII is provided by CTM to NFE. NFE returns a file that discloses whether or not the individual financial transactions posted successfully or encountered posting errors.

FDIC 4C System: CTM provides 4C with two files on a nightly basis; these files contain serviced asset balances and names and ID numbers of active asset servicers. There is no PII contained in these files. 4C provides files to CTM (no PII), as detailed in Section D.3 of this PIA.

6. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface? Has policy or procedures been established for this responsibility and accountability? Explain.

   While the DRR CTM Program Manager/Data Owner ultimately is responsible, all users of the system and parties of the interfaces between CTM and NFE, CTM and 4C, and CTM and Service Provider's system are responsible for protecting the privacy rights of the public and employees affected by the interface. The policy and procedures for responsibility and accountability are included in the FDIC's Information Security & Privacy Act Orientation training which includes the General Rules of Behavior that apply to all users of FDIC information resources. All users must agree to abide by these Rules of Behavior before access is granted to FDIC resources and annually thereafter.

7. If other agencies use the data, how will the data be used? Who establishes the criteria for what data can be shared? Have non-disclosure agreements been effected? Explain the purpose for the need to share the data?

   No other agencies use data from the CTM system.

8. Who is responsible for assuring proper use of the data? Is this individual fully accountable should the integrity of the data be compromised? Explain.

   The CTM Program Manager/Data Owner is responsible for the management and decision authority over a specific area of corporate data. The CTM Program Manager/Data Owner and IT Security Manager serve as the source of information for data definition and data protection requirements and are collectively responsible for supporting a corporate-wide view of data sharing. Although the CTM Program Manager/Data Owner and IT Security Manager share this data responsibility, it is every user's responsibility to abide by FDIC data protection rules which are outlined in the FDIC's Information Security & Privacy Act Orientation training courses which all employees take annually and certify that they will abide by the corporation's Rules of Behavior for data protection. This makes it the responsibility of every user to ensure the proper use of corporate data.

9. Explain the magnitude of harm to the corporation if privacy related data is disclosed, intentionally or unintentionally. Would the reputation of the corporation be affected?

   The unauthorized disclosure of data in CTM could have an adverse impact on the Corporation's reputation and is deemed to be a moderate risk. FDIC takes data disclosure very seriously and takes all necessary precautions and security measures to assure the public that such a release will not occur. The security measures and precautions for CTM are regularly reviewed by designated DRR Information Security Unit (ISU) personnel.

10. What involvement will a contractor have with the design and maintenance of the system? Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been developed for contractors who work on the system?

    Contracted developers have the primary responsibility for design, enhancement and maintenance of the CTM system. All individuals who have access to the application complete a Contractor Confidentiality Agreement and Non-Disclosure Agreement on an annual basis. In addition, all contracted staff for CTM use FDIC network accounts and perform all work on FDIC-owned and operated platforms.

11. Explain whether or not the data owner is contacted if it is not clear if other agencies share or have access to the data.

    Other agencies do not share or have access to CTM data.

Accuracy, Timeliness, and Reliability

1. How is the data collected from sources other than FDIC records verified? Has action been taken to determine its reliability that it is virus free and does not contain malicious code? Who is responsible for this making this determination? Explain.

   Data from all external entities (specified in Section D.3 of this PIA) is transferred via an FDIC-furnished mechanism and is validated by software controls to ensure that record counts and totals match. The FDIC has controls in place to ensure that the data is free from viruses and malware. The software controls ensure that all data complies with processing requirements before it is introduced into the CTM application.

2. How will data be checked for completeness? How is this being measured? What is the source for ensuring the completeness of the data? Explain the method used.

   The CTM system is designed to check for required data elements, as well as to check for the completeness of the data files based on control totals provided in header records of the files. If the required information is not provided, or if the contents of the files do not match the hash totals provided by the data source, it will not be processed or stored by the application.

G. 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? Is this part of the system design? Is this documented, if so, where is the document located? Explain.

   The information collected by CTM is necessary to support the functional requirements of the application. The majority of the data elements are required to process financial transactions to the Corporation's General Ledger, which is an essential requirement of the bank closing process, when FDIC has been appointed as Receiver.

2. Will the system derive personal identifiable information from any new data previously non-inclusive, about an individual through aggregation from the information collected? What steps are taken to make this determination? Explain.

   The system does not derive any new PII through the aggregation of data collected.

3. Can the system make privacy determinations about employees that would not be possible without the new data? If so, explain.

   There is no new data from which the system would make any determinations, nor does the CTM application make privacy determinations about users or employees.

4. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use? Does the consolidation of data result in personal identifiable information? Explain.

   The data in CTM is consolidated from several sources, such as interim servicers, external asset servicers, ASPs, etc. (Refer to Section D.3 for a full list of data sources.) To protect the data from unauthorized access or use, the FDIC employs secure, FDIC-furnished transfer mechanisms which are only accessible by users authorized by FDIC. Additionally, access control lists and other technical controls are used to prevent unauthorized access to data. Access is reviewed periodically to ensure that only authorized staff have access to data and that the access is appropriate.

   Furthermore, CTM audit trails record changes to data, identity the user who performed the change, and record when the change was performed.

5. How is the data retrieved? Can it be retrieved by a personal identifier (e.g., social security number)? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

   Data retrievals in CTM is by personal identifiers, such as payor name, ABA routing number, and checking account number, as well as, non-personal identifiers, such as wire/check number, asset ID, or asset name.

6. What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them? Explain how they are distributed.

   No reports are produced on individuals from CTM. All reports are financial in nature, such as a list of financial details that make up a balance in one of the General Ledger accounts. These reports are used to ensure that the accounting for Receiverships and Subsidiaries is proper and in compliance with established policies and procedures. Authorized users and their supervisors have access to the reports.

H. 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? Will the same controls be used? Explain.

   CTM is operated only in one site. All CTM users that create and maintain data in the CTM system are located in FDIC offices, primarily in the Dallas field office.

2. What are the retention periods of data in this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines? Explain.

   The retention periods of data/records are covered by FDIC Records Schedules at: http://fdic01.prod.gov/division/doa/adminservices/records/records/. The Corporation also follows guidance on permanent and temporary records disposition issued by the National Archives and Records Administration (NARA).

3. What are the procedures for disposition of the data at the end of the retention period? How long will any reports produced be maintained? Where are the procedures documented? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)? Who establishes the procedures? Explain.

   Procedures for disposition of the data at the end of the retention period are established in accordance with FDIC Records Schedules at http://fdic01.prod.gov/division/doa/adminservices/records/records/ in conjuction with NARA guidance.

4. Is the system using technologies in ways that the Corporation has not previously employed (e.g., Monitoring software, SmartCards, Caller-ID, biometrics, PIV cards, etc.)? Explain.

   No.

5. How does the use of this technology affect privacy? Does the use of this technology introduce compromise that did not exist prior to the deployment of this technology? Explain.

   There is no new use of technology that would affect privacy.

6. If monitoring is being performed, describe the data being collected. Is monitoring required? If so, describe the need for the monitoring and identify the requirements and explain how the information is protected.

Monitoring is not being performed.

7. If monitoring is not required, explain the controls that will be used to prevent unauthorized monitoring?

   The system is not used to monitor individuals. The system is only accessible by those individuals who have been authorized and then only for the processing location to which they have been associated.

8. In the Federal Register, under which Privacy Act Systems of Record (SOR) does this system operate? Provide number and name.

   The CTM Application operates under FDIC System of Records Notice # 30-64-0013, *Insured Financial Institution Liquidation Records*.

9. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

   Changes to the application may affect functionality but will not impact the overall business processes that the system supports so the Privacy Act System of Records Notice will not require amendment or revision.

I. Business Processes and Technology

1. Does the conduct of this PIA result in circumstances that requires changes to business processes?

   No changes to business processes are required.

2. Does the completion of this PIA potentially result in technology changes?

   No changes to technology is required.