# 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:** | **Mission Capital Advisors** |
| **System Acronym:** | **Mission Capital Advisors** |
| **System Owner/Division or Office:** | **DRR** |
| **Date Approved by Chief Privacy Officer:** | **4/14/2011** |

## 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.

## B. 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.

When a financial institution fails, the Federal Deposit Insurance Corporation (FDIC), in its capacity as "Receiver," assumes the task of collecting and selling the assets (i.e. loans) of the failed financial institution and settling its debts, including claims of deposits in excess of the insured limit. The FDIC either will sell the loans at the time of the financial institution's closing or retain the loans temporarily.

Within FDIC, the Division of Resolutions and Receiverships (DRR) Asset Marketing Branch is responsible for conducting the sales of loans[1] that remain with the Receiver. DRR markets these loans through private "Loan Sale Advisors," who are under contract to perform this service on behalf of the Receiver. FDIC is required to maximize[2] the price of resold assets following a bank failure. The use of Loan Sale Advisors helps FDIC obtain the highest return by tapping into a large pool of potential purchasers or "bidders."

This Privacy Impact Assessment describes the activities involving Mission Capital Advisors ("Mission"), which is one of the Loan Sale Advisors that the FDIC/DRR has contracted with to value and sell assets acquired when a financial institution fails. Mission provides a secure, online website where assets/loan pools may be viewed for purchase by authorized bidders. (Mission currently uses a third-party vendor named Pandesa ShareVault to host the sales portion of its website.)

As part of the loan sale process, Mission collects personally identifiable information (PII) and non-PII from potential bidders who register to participate in the loan sale. Bidders typically are banks or private firms, but in some cases, are individual members of the public, who are required to meet strict eligibility requirements set forth by FDIC and Mission.

Due to the nature of loan sales in the secondary market, Mission must provide potential bidders with all the documents necessary for bidders to conduct appropriate due diligence. These loan sale documents often contain sensitive information, including PII on individual loan customers.

Following a sale, the successful bidder is provided all data through Pandesa ShareVault. Data is removed from the Pandesa ShareVault host website within five months after the sale. Mission retains a copy of the sale information and details in a secure archive

[1] Loan portfolios from failed banks usually contain a variety of performing and non-performing loan products including mortgage, commercial, and consumer loans.

[2] FDIC's mandate is to maximize the price of sold assets following a financial institution failure. Experience has proven that valuations must be performed at the asset-level to validate prices received for assets. The quality and quantity of information available for investor review is critical to receiving the maximum value for the assets.

network folder with restricted access. Backup tapes are encrypted and sent weekly to a secure Iron Mountain facility. All data is deleted, destroyed or expunged upon request from the FDIC.

## C. 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.

   **Bidders**: Mission requires prospective bidders to register on its website before they can access loan sale information containing PII. As part of the registration process, Mission requires prospective bidders to provide the following information: Individual or Business Name; Work Address; Work Phone Number; Fax Number; Tax Identification Number or Social Security Number (SSN); Detailed Company Information (e.g., Number of Employees, Date of Formation, Names/Addresses of Company Owners/Officers/Directors/Trustees/Subsidiaries, etc); Financial Information (e.g., Company's Revenue, Assets, Tangible Net Worth, etc); Proof of Past Loan Purchase Experience; Professional References (Banker, Lawyer and Accountant); Electronic Copies of Articles of Incorporation, Organization, Partnership or similar documentation; and FDIC Security Deposit Agreement.

   **Failed Bank Loan Customers**: PII contained in the entire loan file obtained by the Receiver and shared with Mission may include the following information about individual loan customers: Name, Home Address, Home Email Address, Home Telephone Number, Social Security Number, Tax ID Number, Date of Birth, Place of Birth, Account Number, Account Balance, and other Credit Information. Scanned data may include Driver's License, Tax Returns, Financial Statements, previous and current Credit Reports, Employment History or Information, Employee ID Number, and other data contained in the loan file at the time of the financial institution's closing.

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: Individuals may not opt out of the loan sale process as the FDIC is required to sell all assets acquired from the failed financial institution as soon as possible after the closing of the financial institution. In addition, FDIC is required to receive the highest value possible. To achieve these goals, the FDIC has employed professional Loan Sales Advisors, such as Mission, to value and market these assets. These activities require the availability of all personal information on each asset, in order that bidders may have full access to file content for due diligence.

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

The source of data for the Mission website is the loan/asset data acquired by the Receiver at or following the closing of a financial institution. This data is generally copied from the computer systems of the closed financial institution or its Servicer and securely provided to Mission via secure FTP or encrypted digital media. If files are in hard copy, an authorized subcontractor of FDIC or Mission scans the contents of the loan files to support investor due diligence of all assets offered for sale. These files are scanned either onsite or offsite by the authorized subcontractor. The method for transporting files offsite for scanning adheres to FDIC shipping and security protocols.

After the data has been scanned, Mission performs data validation and organization, re-stacking and labeling all loan documentation in a consistent format to support bidder due diligence. Mission then uploads all loan documentation to its secure, virtual data room ("VDR") hosted by ShareVault. In preparing the loans/loan pools for sale, Mission underwriters supplement asset data, as needed, with a current credit report for the borrower and guarantor (this credit report is ordered by FDIC and provided to Mission), as well as an asset valuation in order to accurately place a value on each asset.

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.

   As explained in Section D.3 of this PIA, the FDIC, in its capacity as Receiver, provides Mission with the loan/asset data that it acquires at or following the closing of a financial institution. This data is used by Mission to value and market these assets, as well as to allow potential bidders to conduct due diligence.

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.

   State and local agencies are not providing data to Mission for use in the valuing and marketing of assets on its website.

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.

   DRR Asset Marketing staff may order a current credit report for a borrower or guarantor from the credit reporting agencies. Mission uses this credit report data to supplement and correctly assess the value of each asset.

**D. 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.

There are four main categories of users:

1. FDIC authorized users, primarily consisting of Division of Resolutions and Receiverships (DRR) Asset Management (AM) staff, who are responsible for the expeditious sale of loans after the failure of a financial institution. AM staff manage and monitor the data being sent to Mission and the sales after data is loaded. In addition, the FDIC Oversight Manager and Technical Monitor in DRR monitor the activities of the staff at Mission.

2. Authorized Mission users, primarily consisting of:
   - Senior Executives/ "Advisory Team Personnel" for purposes of updating data and conducting and monitoring sales of loans/loan pools;
   - Underwriters for the purpose of updating data and preparing the loans/loan pools for viewing by authorized bidders on the Mission website;
   - Administrative staff for the purpose of uploading data to the appropriate portion of the secure website; and
   - Information security/technical staff for the purpose of administering the site and record retention/disposal activities.
   - In addition, authorized subcontractors of Mission may have access to data for the purpose of providing image scanning, research and valuation support to the Mission's Senior Executives/Advisory Team Personnel. Authorized subcontractors, including Pandesa ShareVault, which is the third-party vendor that hosts Mission's sales website, may also have access to the website for purposes of system administration and customer service support (e.g., assisting authorized bidders who may experience technical difficulty in accessing the sales website).

3. Authorized bidders/purchasers for the purpose of reviewing the data in the loans/loan pools as part of the due diligence process and purchasing assets.

4. Other federal government agency personnel, depending on the guarantor or participant to a loan, do not currently have access, but could potentially have access in the future. This may include, for example, the Small Business Administration (SBA), the U.S. Department of Agriculture (USDA), and the Farm Service Agency (FSA).

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.

Access to the data is determined for the four categories of users as follows:

1. FDIC authorized users within DRR, including the Asset Management staff, request access from the contract Oversight Manager in DRR. Access to the

Mission website requires FDIC management approval. Access to the data is limited to those with an operational need to access the information.

2. Authorized Mission users are granted access on a "need-to-know" basis as part of the duties performed for their employer. All Mission employees and authorized subcontractors with access to sensitive data must sign a Confidentiality Agreement and undergo a background investigation. In addition, Mission ensures that individuals are trained on data security and privacy risks, including proper handling of information associated with their activities, and of applicable laws, regulations, policies, and procedures. Access control policies are documented in the Mission Information Security Policy Manual.

3. Authorized bidders/purchasers request access online by registering and agreeing to the Terms of Access. Purchasers' access authorization is subject to the requirements for access provided by the FDIC Oversight Manager and are enforced by Mission.

In order to view loan sale documentation including PII, prospective bidders must complete the registration process as follows:

- Review the Purchaser Eligibility Summary;
- Execute the Confidentiality Agreement;
- Upon submitting the Confidentiality Agreement, an email will be sent to the prospective bidder to complete a Bidder Registration Statement online. (Refer to Section D.1 in this PIA for more information on the detailed data that prospective bidders must provide as part of the registration process.);
- Submit the Bidder Registration Statement along with non-refundable $500 registration processing fee;
- Mission Capital processes the application and verifies references;
- Mission Capital / FDIC approves or denies application for access to confidential information;
- Prospective bidder executes a FDIC security Deposit Agreement and submits a $50,000 refundable deposit directly to the FDIC (if deposit was previously submitted, Mission will verify with FDIC); and
- Prospective bidder receives a login and password for access to the online due diligence website.

4. Other Federal Government Agencies that are guarantors or participants to a loan are not currently accessing the website, but could potentially be granted access in the future on a need-to-know basis, subject to the requirements for access provided by the FDIC Oversight Manager and enforced by Mission. In such a scenario, an agency's access would be limited to only those loans and sales for which they are the guarantor or participant for the purpose of reviewing the status of the sale. Also, a Non-Disclosure Agreement would executed prior to access to the data.

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

Access to the data is restricted based on users "need-to-know" and respective business functions. Only a few administrative users have access to all data. These individuals undergo a rigorous background screening process. Please refer to Sections E.1 and E.2 of this PIA for more information on the access levels and requirements.

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.

   Authorized bidders/purchasers must agree to the Terms of Access and sign Confidentiality Agreements, among other rigorous requirements, as detailed in Sections E.1 and E.2 of this PIA. Authorized Mission employees and authorized subcontractors with access to sensitive data must sign a Confidentiality Agreement and undergo a background investigation. Refer to Section E.2 for more information. Further, access to particular data by Mission employees is segregated and permission-based according to the user's business function and "need to know. Strong passwords are required for access; all authentication is centralized; and all users are centrally provisioned (and removed), which helps prevent rogue users from gaining access to the system without proper authorization.

   In addition, Mission maintains audit trails of all authorized users' access to sales and to assets. Audit trails include such information as the asset reviewed, the user, the date and time. This data is reviewed by the FDIC Oversight Manager or Technical Monitor on an as-needed basis.

   The FDIC Oversight Manager approves access to data by authorized FDIC DRR staff on a need-to-know basis. FDIC employees and contractors must complete a Security Awareness Training and a Corporate Privacy Awareness Orientation 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.

   No FDIC systems share data or have access to the data on the Mission website or network.

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.

   All users are responsible for protecting the privacy of the public and abiding by the terms of the Confidentiality and Non-Disclosure Agreements. Within FDIC/DRR, the Oversight Manager, Technical Monitors, and Program Manager will be responsible for protecting the privacy rights of the public. At Mission, the Information Security Officer (ISO) and Assistant ISO are responsible for

overseeing access and ensuring proper use of data by Mission employees and authorized subcontractors.

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?

   At this time, other government agencies do not have access to loan data on the website. In the future, it is possible that certain agencies that are guarantors of, or participants to, certain loans (e.g., Small Business Administration, the U.S. Department of Agriculture, or Farm Service Agency) may request access to Mission's website in order to determine the status of applicable assets subsequent to the sale. In such a scenario, agencies would only be granted access to those loans and sales applicable to the guarantor or participant for the purpose of reviewing the status of the sale. Also, a Non-Disclosure Agreement would executed prior to access to the data

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 Mission Information Security Officer (ISO) and Assistant ISO are responsible for granting access and ensuring proper use of data by Mission employees and authorized subcontractors. The FDIC Oversight Manager, Technical Monitors and Program Manager are also responsible for assuring proper user of the data. In addition, all users are responsible for protecting the privacy of the public and abiding by the terms of the Confidentiality and Non-Disclosure Agreements.

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?

   While direct harm to the FDIC due to release of data from this website would be limited, if the data in the system were to be compromised, this could potentially have an adverse effect on the reputation of the Corporation and the Corporation's ability to meet its goals of selling assets efficiently and effectively after a bank closing. Therefore, the FDIC/DRR takes all necessary precautions and security measures to assure the public that such a release of data will not occur. These measures are regularly reviewed by the Oversight Manager.

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?

    The Mission website is contractor-owned and maintained. The contractor has signed a Confidentiality Agreement and Non-Disclosure Agreement as part of their contract with the FDIC.

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.

The contract Oversight Manager and/or Technical Monitor would be contacted by the contractor for all clarifications on access to this secure website.

**E. Accuracy, Timeliness, and Reliability**

2. 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 is collected from the asset tracking systems at or maintained for a failed financial institution. The FDIC checks these data for viruses and malicious code before forwarding it to the contractor.

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.

   All available data on each asset is gathered during or subsequent to the closing of a financial institution. As necessary, in order to maximize the price of resold assets following a bank failure, Mission performs data validation, reviewing the loan file for completeness, verifying whether or not certain documents or data is missing, and as feasible updating this data prior to the sale of the loan/loan pool.

**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.

   Yes, the use of the data is both relevant and necessary to the purpose for which Mission's loan sale service/platform was designed. Specifically, the data is necessary in order to value, market and sell assets acquired from closed financial institutions at the highest possible rate of return.

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 website will not derive data. Additional data about each asset is acquired during the valuation process. These data may include a current credit report. Loan Sales Advisors determine whether a credit report is required in order to accurately value an asset.

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

   Not applicable. Employee data is not maintained on this website.

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.

   Not applicable. Data is not consolidated on this website.

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 is retrieved by Loan Sale Number. This is a number assigned by Mission to track each package of assets for sale.

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.

   Reports may be produced for Loan Sales Packages. These reports may include an individual's data, but are not produced on a particular individual.

**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.

   The Mission website is operated in their New York City (NYC) headquarters. Mission currently uses a third-party vendor named Pandesa ShareVault ("ShareVault") to host the data on their sales website. The Pandesa ShareVault data centers are SAS70 Type II certified[3].

   Mission Capital's corporate IT infrastructure is connected via a secure, fully encrypted virtual private network (VPN). Mission's website and the data file host site at Pandesa ShareVault adhere to the Federal Financial Institutions Examination Council (FFIEC) standards including monitored/secured firewalls, Intrusion Detection Systems (IDS) and automatic session time-out and are used to protect the Mission website. Strong passwords are required for access; all authentication is centralized; and all users are centrally provisioned (and removed), which helps prevent rogue users from gaining access to the system without proper authorization. All data is maintained in a secure, monitored facility.

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.

[3] SAS 70 Type II certification is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). SAS 70 represents that a service organization has been through an in-depth audit of their control objectives and control activities, which often include controls over information technology and related processes.

**Individual Loan File Data**: Retention periods for data adhere to FDIC requirements for data retention and to those retention requirements noted in the contract. Following a sale, the successful bidder is provided all data through ShareVault. Data is removed from the ShareVault host website within five months after the sale. Mission retains a copy of the sale information/details for a period of two to seven years. Mission retains a copy of the sale details in a secure, archive network folder with restricted access. Backup tapes are encrypted and sent to a secure Iron Mountain facility. All data is deleted, destroyed or expunged after the two to seven year retention time period, or upon request from the FDIC. Potential bidders/investors who elect to review and download the loan files are required to abide the requirements in the "Confidentiality, Destruction of Documents" clause contained in the FDIC Confidentiality Agreement.

The winning bidders are bound by contract language located in the Confidentiality Agreement, Destruction of Documents clause. When the winning bidder takes possession of the data, the winning bidder's record retention/disposal takes effect and FDIC's record retention requirements no longer apply.

**Bidder Registration Data**: The registration data collected by Mission via its secure website also adheres to FDIC's record retention/disposal policies. Bidder registration data is retained by Mission for purposes of vetting the bidders, recertifying them each year, and notifying them about future loan sales conducted by Mission.

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.

   **Individual Loan Files**: As previously discussed, data returned to the FDIC for storage and disposal is maintained until the records become inactive, at which time they are retired or destroyed in accordance with NARA and FDIC Record Retention and Disposition Schedules. Data retention guidelines are documented in FDIC Directives and Regulations and are followed. Information may be disposed of by shredding, degaussing or overwriting, as applicable for the materials or hardware involved.

   **Potential Bidder/Investor Data**: After a sale is completed, Mission retains bidder data to vet and recertify them, as well as notify them of future loan sales that may be of interest to them. Subsequent marketing communications sent to bidders include an opportunity to opt out of receiving future marketing communications.

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.

Not applicable. The Mission website is not using technologies in ways not previously employed.

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.

   The use of a third-party website to perform online auctions of loans in Receivership may affect privacy. Previously, the marketing of such loans was performed and controlled internally by FDIC, and due diligence was performed at the bank site using hard copy loan files. While using a third-party website may raise privacy issues, both FDIC and Mission have taken appropriate measures, as required by Federal law and regulations, to mitigate potential risks to the data and protect the privacy rights of individuals.

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.

   Not applicable.

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

   Secured firewalls, Intrusion Detection Systems (IDS) and automatic session timeout are in use to ensure unauthorized monitoring does not occur.

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

   FDIC data collected and maintained on behalf of Mission is associated with FDIC System of Record Notice (SORN) Insured Financial Institution Liquidation Records #30-64-0013.

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

   Not applicable.

## I. Business Processes and Technology

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

   No, the conduct of this PIA does not require changes to business processes.

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

No, the completion of this PIA does not result in technology changes.