FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for
Post-Closing Automation and Monitoring (PCAM)

PIA-FDIC-1224

11/21/2019

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

An FDIC Privacy Impact Assessment (PIA) documents and describes the personally identifiable information (PII) the FDIC collects and the purpose(s) for which it collects that information; how it uses the PII internally; whether it shares the PII with external entities, and the purposes for such sharing; whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; how individuals may obtain access to the PII; and how the PII will be protected. The FDIC publishes its PIAs, as well as its System of Records Notices (SORNs), on the FDIC public-facing website[1], which describes FDIC's activities that impact privacy, the authority for collecting PII, and the procedures to access and have PII amended or corrected if necessary.

SYSTEM OVERVIEW

Division of Resolutions & Receiverships (DRR) Asset Management staff uses the Post-Closing Automation and Monitoring (PCAM) application to assign FDIC employees and contractor personnel to loans that will be inventoried when a failed institution goes into receivership. The system monitors and tracks these loans throughout the receivership process.

The FDIC assumes responsibility for servicing these loans, including collecting payments, managing escrow accounts, monitoring delinquencies, managing defaulted loans, funding borrower draw requests under existing lines of credit per contractual obligations under terms of loan documents, and meeting statutory and regulatory requirements that set standards for loan servicing tasks. Retained loan assets are managed and serviced by the FDIC in its receivership capacity on-site at the failed institution's facilities until they are transferred to a national loan servicer via electronic file transfer from the failed institution's servicing platform to the loan servicer's servicing platform. Data about the loans is obtained directly from the institution by FDIC DRR staff as part of the closing process. Also, the former employees, under supervision by FDIC staff with appropriate delegated authority, perform the servicing function described above. DRR Receivership Assistance Services (RAS) contractors act as loan account officers during the interim servicing period, interacting with borrowers, performing special servicing, and generating reports for FDIC.
The previous loan servicing business process was performed using manual procedures and desktop tools. PCAM establishes an automated, centralized and consistent business process and provides tools for internal stakeholders executing and monitoring associated tasks. PCAM allows stakeholders to enter, track, monitor, and update loan servicing status, requests, communications, tasks, approvals, and deliverables. The system has the ability to compile and submit required reports, and visually track, analyze, and display progress toward goals, key performance indicators, and metrics. Personally identifiable information such as Tax Identification number (TIN) and/or Social Security Number (SSN) about the loan borrowers has been added to the system to improve tracking capabilities.

Authorized FDIC employees and contractors access the system through the FDIC network using their FDIC user login/password credentials. Individual loan borrowers are not able to directly make updates within the PCAM application, although borrowers are able to request corrections to loan data by communicating with staff at the failed institution. Additionally, the FDIC allows individuals to correct or amend PII maintained by the FDIC, the procedures for which are published in the SORN(s) listed in Question 2.2 of this PIA.

PRIVACY RISK SUMMARY

In conducting this PIA, FDIC identified potential privacy risks, which are summarized below and detailed in the subsequent sections of this PIA. As indicated, recommendations to mitigate those risks were addressed with stakeholders during the assessment. The privacy risks for this system are categorized within the following privacy functional areas:

- Transparency

[1] www.fdic.gov/privacy

- Minimization
- Data Quality and Integrity

Transparency:
Privacy Risk: Although FDIC makes System of Record Notices and PIAs publicly available on the FDIC.gov website, impacted depositors may not realize their data is being provided to FDIC in conjunction with the failure of their financial institution.

Mitigation: When a financial institution fails, FDIC publishes a notice in the local newspaper(s) about the financial institution failure. In addition, insured financial institutions display the FDIC logo at their physical locations and on their websites.

Minimization:
Privacy Risk: PCAM now collects and maintains Social Security Numbers (SSNs) for identification purposes with regards to loans. Privacy best practice is to remove SSN wherever possible.

Mitigation: PCAM previously operated without utilizing SSN. However, because financial institutions already assign SSN as the identifier for individual loans and customers, the data quality benefits of using SSN in PCAM to ensure accuracy have justified its continued use.

Privacy Risk: A formal records retention process has not yet been documented for PCAM, which could result in records being maintained for a period longer than necessary and enhance the potential for breach of PII in the event of privacy breach and/or security incident.

Mitigation: PCAM is currently in the process of developing an automated data retention process to adhere to the applicable schedule which will be released in the next PCAM version.

Privacy Risk: There is a potential for additional PII to be included within the free text comments fields in loan documentation when incorporated into PCAM.

Mitigation: Authorized PCAM users who access the system and can update the free text comments fields are instructed to only input information that is required for loan tracking purposes. Additionally, system users ensure that only necessary PII to support the business process is collected.

Privacy Risk: During the development of PCAM, production data was placed in the PCAM testing environment for testing purposes, which increases the risk of unauthorized access of PII. Production data, including PII, may not be used outside of the production environment unless a waiver has been approved by management.

Mitigation: A waiver has been approved by DRR management and is currently in place until the data will be removed from the environment. Additionally, appropriate controls have been implemented to safeguard information.

Data Quality and Integrity:
Privacy Risk: Data is not collected directly from individuals. Rather, data is provided by the appropriate financial institution(s) that conduct business with the FDIC.

Mitigation: To ensure data quality and integrity, PCAM prioritizes the direct import of data received from third parties, who originally collected the data from individuals. Additionally, PCAM has processes in place to correct erroneous information at an individual's request as detailed in Section 3.2. No additional mitigation actions are recommended.

Privacy Risk: The system collects/maintains data from failed institutions containing PII. Correcting inaccurate or erroneous information in the system without updating it at the financial institution level will result in the corrections being overwritten.

Mitigation: Where data that contains PII in PCAM was derived from the financial institution, the institution that initially collects the PII has a responsibility and vested interest in ensuring that the PII they collected is

correct to preclude compliance issues with Federal mandates. Individuals should contact their financial institution (under FDIC receivership) directly to correct any erroneous or inaccurate information.

Section 1.0: Information System/Project Description

1.1 What information about individuals, including personally identifiable information (PII) (e.g., name, Social Security number, date of birth, address, etc.) and non-PII, will be collected, used or maintained in the information system or project?

PCAM collects information about loan borrowers, guarantors, participants and details of the loans. Information collected from loan borrowers, guarantors, and participants including: full name; tax identification number (TIN) and/or Social Security Number (SSN); home address; phone number; email address; legal notes; and financial information (which can include items such as loan number and loan amount).

Additionally, information is collected on FDIC employees and contractors, who serve as users of the system. Information collected includes: full name; user name; work phone number and work email address.

PII Element	Yes	No
Full Name	☒	☐
Date of Birth	☐	☒
Place of Birth	☐	☒
Social Security Number	☒	☐
Employment Status, History or Information	☐	☒
Mother's Maiden Name	☐	☒
Certificates (e.g., birth, death, naturalization, marriage, etc.)	☐	☒
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	☐	☒
Home Address	☒	☐
Phone Number(s)	☒	☐
Email Address	☒	☐
Employee Identification Number (EIN)	☐	☒
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	☒	☐
Driver's License/State Identification Number	☐	☒
Vehicle Identifiers (e.g., license plates)	☐	☒
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	☒	☐
Education Records	☐	☒
Criminal Information	☐	☒
Military Status and/or Records	☐	☒
Investigation Report or Database	☐	☒
Biometric Identifiers (e.g., fingerprint, voiceprint)	☐	☒
Photographic Identifiers (e.g., image, x-ray, video)	☐	☒
Other (Specify: _____)	☐	☒

1.2 Who/what are the sources of the PII in the information system or project?

Data Source	Description of Information Provided by Source

Failing/Failed Financial Institutions (FI)/ via Business Information System(BIS) Loan Database named PCAM Data	Receivership loan data including loan holder Tax ID (may be SSN), contact information, financial information, and legal notes(notes from the lawyer assigned to cases, related to various legal proceedings)
Enterprise Data Warehouse (EDW) Person Master Database	FDIC employee and contractor staff information including full name, user name, FDIC work phone and FDIC work email
Asset Management staff Manual Entry	Manually Entered Data by FDIC DRR staff or contractors related to the receivership, including: name, location, bank certification number, Financial Institution Number, phone number for the site, status codes, start and end date, inventory type, and vendor name of the contractor staff. Also, specific loan data elements not contained in the institution's loan servicing platform - during the physical loan file inventory, RAS contractors will enter borrower, guarantor, participant, and collateral information into PCAM. They will then update or correct information if needed.

1.3 Has an Authority to Operate (ATO) been granted for the information system or project?

PCAM completed a change driven security control assessment on 11/15/2019. It is a sub-system within the authorization boundary of the Enterprise Data Management (EDM) which received its Authorization to Operate (ATO) on 10/21/2011.

Section 2.0: Transparency

Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

2.1 How does the agency revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change?

Through the conduct, evaluation and review of PIAs and SORNs, the FDIC ensures notices are revised to reflect changes in practice or policy that affect PII or changes in activities that may impact Privacy as soon as practicable.

2.2 In the Federal Register, under which Privacy Act System of Record Notice (SORN) does this information system or project operate? Provide number and name.

The following SORN(s) apply to the PCAM: FDIC-30-64-0013 "Insured Financial Institution Liquidation Records" in which records are maintained to support the receivership, conservatorship, and other resolution functions of the FDIC authorized by applicable Federal and state statutes.

2.3 If the information system or project is being modified, will the Privacy Act SORN require amendment or revision? Explain.

Changes to PCAM may require amendments to the Privacy Act SORN; however, there are no changes at this time that affect the SORN. Generally, the FDIC conducts reviews of its SORNs every three years and, if needed, the Privacy Act SORN will be updated at that time.

2.4 If a Privacy Act Statement is required, how is the Privacy Act Statement provided to individuals before collecting their PII? (The Privacy Act Statement provides formal notice to individuals of the authority to collect PII, the purpose for collection, intended uses of the information and the consequences of not providing the information.) Explain.

PCAM receives data on loan borrowers, guarantors, and participants from third-parties. As a result, the FDIC does not have the ability to provide Privacy Act Statements or privacy notices prior to the Agency's processing of these individuals' PII. Additionally, this PIA serves as notice of the information collection.

For authorized PCAM users who log into the system, an FDIC Privacy Act Statement is provided at the login screen. Additionally, this PIA and the SORN(s) listed in 2.2 serve as notice of the information collection.

2.5 How does the information system or project ensure that its privacy practices are publicly available through organizational websites or otherwise? How does the information system or project ensure that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)? Explain.

The FDIC Privacy Program page contains policies and information related to SORNs, PIAs, FDIC's Privacy Policy, and contact information for the SAOP, the Privacy Program Manager, the Privacy Act System of Records Clearance Officer, and the Privacy Program (Privacy@fdic.gov). See https://www.fdic.gov/privacy.

Privacy Risk Analysis: Related to Transparency

Privacy Risk: Although FDIC makes System of Record Notices and PIAs publicly available on the FDIC.gov website, impacted depositors may not realize their data is being provided to FDIC in conjunction with the failure of their financial institution.

Mitigation: When a financial institution fails, FDIC publishes a notice in the local newspaper(s) about the financial institution failure. In addition, insured financial institutions display the FDIC logo at their physical locations and on their websites.

Section 3.0: Access and Amendment

Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.

3.1 What are the procedures that allow individuals to access their information?

PCAM receives data on loan borrowers, guarantors, and participants provided by failed financial institutions which may include information about financial institution customers or employees in conjunction with FDIC's examination and supervision authorities. Individuals should contact the appropriate financial institution (under FDIC receivership) directly to access their information.

Additionally, the FDIC allows individuals to access PII maintained by the FDIC, the procedures for which are published in the SORN(s) listed in Question 2.2 of this PIA.

3.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

PCAM receives data on loan borrowers, guarantors, and participants provided by financial institutions who are regulated by FDIC, which may include information about financial institution customers or employees in conjunction with FDIC's examination and supervision authorities. Individuals should contact the appropriate financial institution (under FDIC receivership) directly to correct any erroneous or inaccurate information. By following this process, any changes made to the data by the individual at the financial institution level will flow directly into PCAM.

Additionally, the FDIC allows individuals to correct or amend PII maintained by the FDIC, the procedures for which are published in the SORN(s) listed in Question 2.2 of this PIA.

3.3 How does the information system or project notify individuals about the procedures for correcting their information?

The FDIC has a process for disseminating corrections or amendments of collected PII to other authorized users, the procedures for which are published in the SORN, listed in Question 2.2 of this PIA. This is in accordance with the Privacy Act and FDIC Circular 1031.1.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: There are no identifiable risks with Access and Amendment for PCAM.

Mitigation: No mitigation actions are recommended.

Section 4.0: Accountability

Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.

4.1 Describe how FDIC's governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy.

FDIC maintains a risk-based, enterprise-wide privacy program that is based upon sound privacy practices. The FDIC Privacy Program is compliant with all applicable laws and is designed to build and sustain public trust, protect and minimize the impacts on the privacy of individuals, while also achieving the FDIC's mission.

The FDIC Privacy Program is led by the FDIC's Chief Information Officer (CIO) and Chief Privacy Officer (CPO), who also has been designated as FDIC's Senior Agency Official for Privacy (SAOP). The CIO/CPO reports directly to the FDIC Chairman, and is responsible for ensuring compliance with applicable federal privacy requirements, developing and evaluating privacy policy, and managing privacy risks. The program ensures compliance with federal privacy law, policy and guidance. This includes the Privacy Act of 1974, as amended; Section 208 of the E-Government Act of 2002, Section 522 of the 2005 Consolidated Appropriations Act, Federal Information Security Modernization Act of 2014, Office of Management and Budget (OMB) privacy policies, and standards issued by the National Institute of Standards and Technology (NIST).

The FDIC's Privacy Program Staff supports the SAOP in carrying out those responsibilities through the management and execution of the FDIC's Privacy Program. The Privacy Program has been fully integrated throughout the agency and is supported on a part-time basis by divisional Information Security Managers located within the agency's divisions and offices.

4.2 Describe the FDIC privacy risk management process that assesses privacy risks to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.

Risk analyses are an integral component of FDIC's Privacy program. Privacy risks for new and updated collections of PII are analyzed and documented in Privacy Threshold Analyses (PTAs) and PIAs. A PTA is used to determine whether a PIA is required under the E-Government Act of 2002 and the Consolidated Appropriations Act of 2005. A PIA is required for: (1) a new information technology (IT) system developed or procured by FDIC that collects or processes PII; (2) a substantially changed or modified system that may create a new privacy risk; (3) a new or updated rulemaking that may affect the privacy of PII in some manner; or (4) any other internal or external electronic collection activity or process that involves PII.

4.3 Does this PIA capture privacy risks posed by this information system or project in accordance with applicable law, OMB policy, or any existing organizational policies and procedures?

Privacy risks posed by the information system or project are captured in PIAs, when conducted in accordance with applicable law, OMB policy, and FDIC policy (Circular 1360.19). PIAs are posted on FDIC's public-facing website, https://www.fdic.gov/privacy.

4.4 What roles, responsibilities and access will a contractor have with the design and maintenance of the information system or project?

The FDIC has been working with contractors to design and develop the system and contractors may be employed to provide support and maintenance for this system.

Due to the contractors' access to PII, contractors are required to take mandatory annual information security and privacy training. Privacy and security related responsibilities are specified in contracts and associated Risk Level Designation documents. Privacy-related roles, responsibilities, and access requirements are documented in relevant PIAs.

4.5 Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been completed and signed for contractors who work on the information system or project? Are privacy requirements included in the contract?

Yes, Confidentiality Agreement has been completed and signed for contractors who work on the information system or project. Privacy and security requirements for contractors and service providers are mandated and are documented in relevant contracts.

4.6 How is assurance obtained that the information in the information system or project is used in accordance with the practices described in this PIA and, if applicable, the associated Privacy Act System of Records Notice?

Through the conduct, evaluation and review of PIAs and SORNs, the FDIC monitors and audits privacy controls. Internal privacy policies are reviewed and updated as required. The FDIC Privacy Program is currently in the process of implementing a Privacy Continuous Monitoring (PCM) program in accordance with OMB Circular A-130.

4.7 Describe any privacy-related training (general or specific) that is provided to users of this information system or project.

The FDIC Privacy Program maintains an ongoing Privacy Training Plan that documents the development, implementation, and update of a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures. Annual Security and Privacy Training is mandatory for all FDIC employees and contractors and they are required to electronically certify their acceptance of responsibilities for privacy requirements upon completion. Specified role-based privacy training sessions are planned and provided by the FDIC Privacy Program staff as well.

4.8 Describe how the FDIC develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

The FDIC Privacy Program develops reports both for internal and external oversight bodies through several methods, including the following: Annual Senior Agency Official for Privacy Report (SAOP) as required by FISMA; weekly reports to the SAOP; bi-weekly reports to the CISO, monthly meetings with the SAOP and CISO; Information Security Manager's Monthly meetings.

4.9 Explain how this information system or project protects privacy by automating privacy controls?

Privacy has been integrated within the FDIC Systems Development Life Cycle (SDLC), ensuring that stakeholders are aware of, understand, and address Privacy requirements throughout the SDLC, including the automation of privacy controls if possible. Additionally, FDIC has implemented technologies to track, respond, remediate and report on breaches, as well as to track and manage PII inventory.

4.10 Explain how this information system or project maintains an accounting of disclosures held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made?

The FDIC maintains an accurate accounting of disclosures of information held in each system of record under its control, as mandated by the Privacy Act of 1974 and FDIC Circular 1031.1 Disclosures are tracked and managed using FOIAExpress.

4.11 Explain how the information system or project retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer?

The FDIC retains the accounting of disclosures as specified by the Privacy Act of 1974 and FDIC Circular 1031.1.

4.12 Explain how the information system or project makes the accounting of disclosures available to the person named in the record upon request?

The FDIC makes the accounting of disclosures available to the person named in the record upon request as specified by the Privacy Act of 1974 and FDIC Circular 1031.1.

Privacy Risk Analysis: Related to Accountability

Privacy Risk: There are no identifiable risks associated with accountability for PCAM.

Mitigation: No mitigation actions are recommended.

Section 5.0: Authority

Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.

5.1 Provide the legal authority that permits the creation, collection, use, processing, storage, maintenance, dissemination, disclosure and/or disposing of PII within the information system or project. For example, Section 9 of the Federal Deposit Insurance Act (12 U.S.C. 1819).

The FDIC ensures that collections of PII are legally authorized through the conduct and documentation of PIAs and the development and review of SORNs. FDIC Circular 1360.20 'FDIC Privacy Program' mandates that the collection of PII be in accordance with Federal laws and guidance. This particular system or project collects PII pursuant to the following laws:

• 12 U.S.C. 1821: deals with Deposit Insurance, the Deposit Insurance Fund and closing and resolving banks. The Corporation shall insure the deposits of all insured depository institutions as provided in this chapter.
• 12 U.S.C. 1822: deals with FDIC as a Receiver of failed banks
• Executive Order 9397: stipulates the requirement for the use of SSNs by President Roosevelt
• 12 CFR 366: deals with FDIC contractors

Privacy Risk Analysis: Related to Authority

Privacy Risk: There are no identifiable privacy risks related to authority, as FDIC ensure that collection of personally identifiable information(PII) are legally authorized through the conduct and documentation of Privacy Impact Assessment (PIA) and the development and review of System of Records (SORNs).

Mitigation: No mitigation actions are recommended.

Section 6.0: Minimization

Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.

6.1 How does the information system or project ensure that it has identified the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection?

The DRR Asset Management Section has required business processes that it must follow when assets are retained by the FDIC. These include, but are not limited to: inventorying loan documents retained by the FDIC; communicating with borrowers and other stakeholders of retained loans about FDIC's plans regarding their loans; resolving contingent liabilities related to retained loans; and performing interim servicing on retained loans. Each business process requires access to borrower and stakeholder PII to complete; for example, developing communication with borrowers requires access to borrower names and addresses. PCAM automates and centralizes these processes, and the collection of PII reflects the minimum amount needed to complete each discrete business process conducted post-failure.

FDIC DRR has identified the minimum PII elements required to meet the purposes of the system as listed in Question 9.1 of this PIA. PCAM users ensure that only the fields necessary to support business processes are included in intake date, and subsequently ensure that any open text fields do not include additional personally identifiable information.

Additionally, through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that the collection of PII is relevant and necessary to accomplish the legally authorized purpose for which it is collected.

6.2 How does the information system or project ensure limits on the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent?

Although there are no automated data retention processes in the current system release, data in the system falls under the FDIC DRR's Records Retention Schedule for Open Bank Data (RAR1010) and Closed Bank Data (RAR1030). PCAM is currently in the process of developing an automated data retention process to adhere to the applicable schedule which will be released in the next PCAM version.

Additionally, through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that the collection and retention of PII is limited to the PII that has been legally authorized to collect.

6.3 How often does the information system or project evaluate the PII holding contained in the information system or project to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose?

FDIC maintains an inventory of systems that contain PII. On a semi-annual basis, FDIC does an evaluation of information in the system to ensure it is the same as in the PIA and not kept longer than its retention period. New collections are evaluated to see if they are part of the inventory.

6.4 What are the retention periods of data in this information system? or project? What are the procedures for disposition of the data at the end of the retention period? Under what guidelines are the retention and disposition procedures determined? Explain.

Data in the system falls under DRR's Records Retention Schedule for Open Bank Data (RAR1010) and Closed Bank Data (RAR1030). PCAM is currently in the process of developing an automated data retention process to adhere to the applicable schedule which will be released in the next PCAM version.

Additionally, records are retained in accordance with the FDIC Circular 1210.1 FDIC Records and Information Management Policy Manual and National Archives and Records Administration (NARA)-approved record retention schedule. Information related to the retention and disposition of data is captured and documented within the PIA process. The retention and disposition of records, including PII, is addressed in Circulars 1210.1 and 1360.9.

6.5 What are the policies and procedures that minimize the use of PII for testing, training, and research? Does the information system or project implement controls to protect PII used for testing, training, and research?

Use of sensitive data outside the production environment requires the management approval via a waiver. Currently, some PII is utilized in the PCAM production environment. A waiver has been approved by DRR management, and appropriate controls have been put in place.

Privacy Risk Analysis: Related to Minimization

Privacy Risk: PCAM now collects and maintains Social Security Numbers (SSNs) for identification purposes with regards to loans. Privacy best practice is to remove SSN wherever possible.

Mitigation: PCAM previously operated without utilizing SSN. However, because financial institutions already assign SSN as the identifier for individual loans and customers, the data quality benefits of using SSN in PCAM to ensure accuracy have justified its continued use.

Privacy Risk: A formal records retention process has not yet been documented for PCAM, which could result in records being maintained for a period longer than necessary and enhance the potential for breach of PII in the event of privacy breach and/or security incident.

Mitigation: PCAM is currently in the process of developing an automated data retention process to adhere to the applicable schedule which will be released in the next PCAM version.

Privacy Risk: There is a potential for additional PII to be included within the free text comments fields in loan documentation when incorporated into PCAM.

Mitigation: Authorized PCAM users who access the system and can update the free text comments fields are instructed to only input information that is required for loan tracking purposes. Additionally, system users ensure that only necessary PII to support the business process is collected.

Privacy Risk: During the development of PCAM, production data was placed in the PCAM testing environment for testing purposes, which increases the risk of unauthorized access of PII. Production data, including PII, may not be used outside of the production environment unless a waiver has been approved by management.

Mitigation: A waiver has been approved by DRR management and is currently in place until the data will be removed from the environment. Additionally, appropriate controls have been implemented to safeguard information.

Section 7.0: Data Quality and Integrity

Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual

7.1 Describe any administrative and technical controls that have been established to ensure and maximize the quality, utility, and objectivity of PII, including its accuracy, relevancy, timeliness, and completeness.

The FDIC reviews privacy artifacts for adequate measures to ensure the accuracy, relevance, timeliness, and completeness of PII in each instance of collection or creation.

7.2 Does the information system or project collect PII directly from the individual to the greatest extent practicable?

PCAM receives data on loan borrowers, guarantors, and participants from third-parties. Additional PII is maintained on employees and contractors who enter information manually in PCAM as listed in Section 1.1. The FDIC reviews privacy artifacts to ensure each collection of PII is directly from the individual to the greatest extent practicable.

7.3 Describe any administrative and technical controls that have been established to detect and correct PII that is inaccurate or outdated.

The FDIC reviews privacy artifacts to ensure adequate measures to check for and correct any inaccurate or outdated PII in its holdings.

7.4 Describe the guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

The FDIC's guidelines for the disclosure of information subject to Privacy Act protections are found in Part 310 of the FDIC Rules and Regulations.

7.5 Describe any administrative and technical controls that have been established to ensure and maximize the integrity of PII through security controls.

Through its PTA adjudication process, the FDIC Privacy Program utilizes the Federal Information Processing Standards Publication 199 (FIPS 199) methodology to determine the potential impact on the FDIC and individuals should there be a loss of confidentiality, integrity, or availability of the PII. The Office of the Chief Information Security Officer prescribes administrative and technical controls for the system or project based on the FIPS 199 determination.

7.6 Does this information system or project necessitate the establishment of a Data Integrity Board to oversee a Computer Matching Agreements and ensure that such an agreement complies with the computer matching provisions of the Privacy Act?

The FDIC does not maintain any Computer Matching Agreements under the Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988, and consequently does not have a need to establish a Data Integrity Board.

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: Data is not collected directly from individuals. Rather, data is provided by the financial institutions regulated by FDIC that conduct business with the FDIC.

Mitigation: To ensure data quality and integrity, PCAM prioritizes the direct import of data received from third parties, who originally collected the data from individuals. Additionally, PCAM has processes in place to correct erroneous information at an individual's request as detailed in Section 3.2. No additional mitigation actions are recommended.

Privacy Risk: The system collects/maintains data from failed institutions containing PII. Correcting inaccurate or erroneous information in the system without updating it at the financial institution level will result in the corrections being overwritten.

Mitigation: Where data that contains PII in PCAM was derived from the financial institution, the institution that initially collects the PII has a responsibility and vested interest in ensuring that the PII they collected is correct to preclude compliance issues with Federal mandates. Individuals should contact their financial institution (under FDIC receivership) directly to correct any erroneous or inaccurate information.

Section 8.0: Individual Participation

Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.

8.1 Explain how the information system or project provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection.

PCAM receives data on loan borrowers, guarantors, and participants from third-parties. As a result, the FDIC does not have the ability to provide Privacy Act Statements or privacy notices prior to the Agency's processing of these individuals' PII. Additionally, this PIA serves as notice of the information collection.

For authorized PCAM users who log into the system, an FDIC Privacy Act Statement is provided at the login screen. Additionally, this PIA and the SORN(s) listed in 2.2 serve as notice of the information collection.

8.2 Explain how the information system or project provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII.

PCAM receives data on loan borrowers, guarantors, and participants from third-parties. As a result, the FDIC does not have the ability to provide Privacy Act Statements or privacy notices prior to the Agency's processing of these individuals' PII. Additionally, this PIA serves as notice of the information collection.

For authorized PCAM users who log into the system, an FDIC Privacy Act Statement is provided at the login screen. Additionally, this PIA and the SORN(s) listed in 2.2 serve as notice of the information collection.

8.3 Explain how the information system or project obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII.

It is not feasible or appropriate to get direct consent prior to any new use or disclosures of previously collected PII. If applicable, the FDIC Privacy Program will update the relevant Privacy Act SORN(s) as well as the relevant PIA.

8.4 Explain how the information system or project ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

PCAM receives data on loan borrowers, guarantors, and participants from third-parties. As a result, the FDIC does not have the ability to provide Privacy Act Statements or privacy notices prior to the Agency's processing of these individuals' PII. Additionally, this PIA serves as notice of the information collection.

8.5 Describe the process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices?

The FDIC Privacy Program website, https://www.fdic.gov/privacy, instructs viewers to direct privacy questions to the FDIC Privacy Program through the Privacy@FDIC.gov email address. Complaints and questions are handled on a case-by-case basis.

Privacy Risk Analysis: Related to Individual Participation

Privacy Risk: There are no identifiable risks associated with individual participation for PCAM.

Mitigation: No mitigation actions are recommended.

Section 9.0: Purpose and Use Limitation

Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

9.1 Describe the purpose(s) for which PII is collected, used, maintained, and shared as specified in the relevant privacy notices.

The system uses PII to accomplish the following purposes: track, monitor, and update the status of loans serviced by FDIC following the closing or failing of a financial institution; to compile and submit required reports; to visually track, analyze, and display progress regarding metrics or KPIs; and to communicate tasks and approvals related to loans.

9.2 Describe how the information system or project uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices? Who is responsible for assuring proper use of data in the information system or project and, if applicable, for determining what data can be shared with other parties and information systems? Have policies and procedures been established for this responsibility and accountability? Explain.

Through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that PII is only used for authorized uses internally in accordance with the Privacy Act and FDIC Circular 1360.9 "Protecting Sensitive Information" with the use of various privacy controls.

Additionally, annual Information Security and Privacy Awareness Training are mandatory for all staff and contractors, which include information on rules and regulations regarding the sharing of PII with third parties. PCAM Data Owners/System Managers, Technical Monitors, Oversight Mangers, and Information Security Managers are collectively responsible for assuring proper use of data.

Specific training for the system is being developed to address specific functions and responsibilities.

9.3 How is access to the data determined and by whom? Explain the criteria, procedures, security requirements, controls, and responsibilities for granting access.

User roles and security are handled by the Workspace Management System, which is a DRR application. The system employs restrictions on personnel authorized to input information into the system by using a role-based access control environment.

The following steps are taken to ensure only authorized personnel have access to the system and that the authorized personnel are restricted to their specific role functions:

1. To access the system, all users must complete an FDIC provisioning software request for their assigned role.
2. DRR Security monitors/audits all user access to the system, ensuring that only active/approved users retain access.

9.4 Do other internal information systems receive data or have access to the data in the information system? If yes, explain.

☒ No
☐ Yes Explain.

9.5 Will the information system or project aggregate or consolidate data in order to make determinations or derive new data about individuals? If so, what controls are in place to protect the newly derived data from unauthorized access or use?

The system will not aggregate or consolidate data to make determinations or derive new data about individuals.

9.6 Does the information system or project share PII externally? If so, is the sharing pursuant to a Memorandum of Understanding, Memorandum of Agreement, or similar agreement that specifically describes the PII covered and enumerates the purposes for which the PII may be used. Please explain.

Retained loan asset information along with the demographic and financial data on the loan and the loan collateral is shared with National Loan Servicers. Additionally, selected loan demographic and collateral information are shared with the loan purchasers. National Loan Servicers are contracted through the FDIC Receivership Basic Ordering Agreements process which includes stringent data security and privacy requirements per FDIC contracting policy. Contracts and agreements for these services are managed by DRR Contract Officers and Oversight Managers. Loan purchasers are required to execute confidentiality agreements prior to being given access to any loan information, during the bidding process. When a bidder acquires a loan, a Loan Sale Agreement is completed, which requires the execution of a Confidentiality Agreement prior to being granted access to the loan information.

Additionally, through the conduct, evaluation and review of PIAs and SORNs, the FDIC ensures that PII shared with third parties is used only for the authorized purposes identified or for a purpose compatible with those purposes, in accordance with the Privacy Act of 1974, FDIC Circular 1031.1 'Administration of the Privacy Act', and FDIC Circular 1360.17 'Information Technology Security Guidance for FDIC Procurements/Third Party Products'. The FDIC also ensures that agreements regarding the sharing of PII with third parties specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used, in accordance with FDIC Circular 1360.17 and FDIC Circular 1360.9

9.7 Describe how the information system or project monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII.

Annual Information Security and Privacy Awareness Training are mandatory for all staff and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

9.8 Explain how the information system or project evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

The FDIC reviews privacy artifacts to evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Privacy Risk Analysis: Related to Use Limitation

Privacy Risk: There is no identifiable privacy risks associated with use limitation.

Mitigation: No mitigation actions are recommended.

Section 10.0: Security

Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

10.1 Describe the process that establishes, maintains, and updates an inventory that contains a listing of all information systems or projects identified as collecting, using, maintaining, or sharing PII.

FDIC maintains an inventory of systems that contain PII. On a semi-annual basis, FDIC does an evaluation of information in the system to ensure it is the same as in the PIA and not kept longer than its retention period. New collections are evaluated to see if they are part of the inventory.

10.2 Describe the process that provides each update of the PII inventory to the CIO or information security official to support the establishment of information security requirements for all new or modified information systems or projects containing PII?

The FDIC Privacy Program updates the Chief Information Security Officer (CISO) on PII holdings via the PTA adjudication process. As part of the PTA adjudication process, the FDIC Privacy Program reviews the system or project's FIPS 199 determination. The FDIC Privacy Program will recommend the appropriate determination to the CISO should the potential loss of confidentiality be expected to cause a serious adverse effect on individuals.

10.3 Has a Privacy Incident Response Plan been developed and implemented?

FDIC has developed and implemented a Breach Response Plan in accordance with OMB M-17-12.

10.4 How does the agency provide an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan?

Responses to privacy breaches are addressed in an organized and effective manner in accordance with the FDIC's Breach Response Plan.

Privacy Risk Analysis: Related to Security

Privacy Risk: There are no identifiable privacy risks associated with security for PCAM.

Mitigation: No mitigation actions are recommended.