FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)

for

Division of Risk Management Supervision (RMS)

File Image Viewer for Examinations (FIVE)

Date Approved by Chief Privacy Officer (CPO)/Designee:
9/21/2018

Section 1.0: Introduction

In accordance with federal regulations and mandates[1], the FDIC conducts Privacy Impact Assessments (PIAs) on systems, business processes, projects and rulemakings that involve an *electronic* collection, creation, maintenance or distribution of personally identifiable information (PII).[2] The objective of a Privacy Impact Assessment is to identify privacy risks and integrate privacy protections throughout the development life cycle of an information system or electronic collection of PII. A completed PIA also serves as a vehicle for building transparency and public trust in government operations by providing public notice to individuals regarding the collection, use and protection of their personal data.

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.

Upon completion of this questionnaire and prior to acquiring signatures, please email the form to the FDIC Privacy Program Staff at: privacy@fdic.gov, who will review your document, contact you with any questions, and notify you when the PIA is ready to be routed for signatures.

Section 2.0: System/Project Description

2.1 In this section of the Privacy Impact Assessment (PIA), describe the system/project and the method used to collect, process, and store information. Additionally, include information about the business functions the system/project supports.

The File Image Viewer for Examinations (FIVE) application is a file image viewer that allows examiners to view imaged loan documents that are securely transferred from participating financial institutions (FIs) or Technology Service Providers (TSPs) in order to conduct loan reviews. It uses an xml document, containing indexing metadata, to render the user interface. From their PC or laptop, users launch a local "website" to view the files. The website runs only on the client machine and does not run on the FDIC network or the World Wide Web. Data will be in the form of imaged loan documents received from FIs and TSPs as requested by the FDIC. FIVE has been internally developed by the FDIC's Division of Risk Management Supervision (RMS).

[1] Section 208 of the E-Government Act of 2002 requires federal government agencies to conduct a Privacy Impact Assessment (PIA) for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information (PII). Office of Management and Budget (OMB) Memorandum M-03-22 provides specific guidance on how Section 208 should be implemented within government agencies. The Privacy Act of 1974 imposes various requirements on federal agencies whenever they collect, create, maintain, and distribute records that can be retrieved by the name of an individual or other personal identifier, regardless of whether the records are in hardcopy or electronic format. Additionally, Section 522 of the 2005 Consolidated Appropriations Act requires certain Federal agencies to ensure that the use of technology sustains, and does not erode, privacy protections, and extends the PIA requirement to the rulemakings process.

[2] For additional guidance about FDIC rulemaking PIAs, visit the Privacy Program website or contact the FDIC Privacy Program Staff at privacy@fdic.gov.

Section 3.0: Data in the System/Project

The following questions address the type of data being collected and from whom (nature and source), why the data is being collected (purpose), the intended use of the data, and what opportunities individuals have to decline to provide information or to consent to particular uses of their information.

3.1 What personally identifiable information (PII) (e.g., name, social security number, date of birth, address, etc.) will be collected, used or maintained in the system? Explain.

FIVE enables examination staff to view imaged loan documents during an exam. These documents may include the following types of PII: full name; date of birth; Social Security number (SSN); photographic identifiers; driver's license/state identification number; employee identification number; vehicle identifiers; home address; non-work phone numbers; financial and income information or numbers; certificates of birth, death, marriage, naturalization, or marriage; legal documents or records, such as divorce records or criminal records; investigation reports; Web URLs; non-work email addresses; education records; military status and/or records; employment status and/or records; and foreign activity or interest reports. The aforementioned PII may pertain to the following categories of individuals: FI customers.

3.2 What is the purpose and intended use of the information you described above in Question 3.1?

The information specified in Question 3.1 is necessary to support the examination and oversight functions of the FDIC. Specifically, the information is used to assess the FI and/or FI staff viability, conformance with regulations, applications, etc., in order to avoid a negative impact to the insurance fund. Loan, deposit, and other FI records are reviewed directly to help determine the viability of an institution's underlying assets as well as compliance with consumer regulations. While the PII obtained from applicants is used to determine their credit worthiness,[3] most other PII contained within FIVE is typically non-sensitive and/or part of broader documentation used to supervise the institution (e.g. a loan agreement has a borrower's address on it, but the agreement is used to support the borrower's obligation to the bank). Sensitive PII, such as a SSN, is used by financial institutions to run credit checks for applicants.

3.3 If Social Security Numbers (SSNs) are collected, used, or maintained in the system, please answer the following:

a) Explain the business purpose/need requiring the collection of SSNs: As part of the FDIC's examination and supervision mission, FIVE facilitates the distribution and temporary storage of loan image documents, some of which may contain SSNs. SSNs are not commonly obtained, but if needed directly (or if embedded in more important information), they are used to obtain credit reports or for other investigatory purposes. The collection of SSNs is incidental to the distribution and temporary storage for loan image documents, and is not required for the scope of work being conducted.

b) Aside from 12 U.S.C. § 1819, which provides the general authority for the Corporation to collect SSNs, are there any other Federal statutes/authorities that justify the collection and/or use of SSNs?

☒ Yes List any additional legal authorities:
12 U.S.C. § 1820, et. seq. The collection of SSNs is incidental to the document distribution and temporary storage of loan image documents, and is not required for the scope of work being conducted.

☐ No

c) Is the SSN is masked or otherwise truncated within the system?

☐ Yes. Explain:

☒ No. Is it possible to mask or otherwise truncate the SSN within the system?

☐ Yes. Explain how it may be masked or truncated and why this has not been implemented:

☒ No. Explain why it may not be masked or truncated: The imaged loan documents used by FIVE are not altered as they represent official loan documents that support FDIC's position if any eventual legal actions are brought forth.

[3] As alluded to previously, all information used to determine credit-worthiness is collected from the institution.

d) Is access to SSNs (and other sensitive PII) restricted in any way to specific groups of users of the system?

☒ Yes. Explain: Loan image files that may contain SSNs and other sensitive PII are restricted to examination staff by region. Examination staff must be assigned to the region where the exam is being conducted.

☐ No. Is it possible to restrict access to specific groups of users within the system?

☐ Yes. Explain how access may be restricted and why this has not been implemented:

☐ No. Explain why access cannot be restricted:

3.4 Who/what are the sources of the information in the system? How are they derived?

Loan image files are sourced from participating FI/TSP loan imaging systems.[4] The files are securely transferred to the FDIC via Globalscape, a secure file transfer tool.

3.5 What Federal, state, and/or local agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

No other Federal, state or local agencies provide data for use in the system.

3.6 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.

Loan image files are sourced from participating FI/TSP loan imaging systems. These files are used strictly for the purpose of loan review as part of the examination process.

3.7 Do individuals have the opportunity to decline to provide personal information and/or consent only to a particular use of their data (e.g., allowing basic use of their personal information, but not sharing with other government agencies)?

☒ No Explain: FIVE does not collect any data directly from individuals. Information is gathered through examination and supervision activities of the FDIC.

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

Section 4.0: Data Access and Sharing

The following questions address who has access to the data, with whom the data will be shared, and the procedures and criteria for determining what data can be shared with other parties and systems.

4.1 Who will have access to the data in the system (internal and external parties)? Explain their purpose for having access to this information.

FDIC RMS and Division of Depositor and Consumer Protection (DCP) field examiners, the RMS FIVE administrative team, and RMS/DCP field management will have access to information in FIVE to conduct loan reviews in support of their oversight responsibility. Authorized FDIC Division of Information Technology (DIT) system administrators will have access to FIVE for purposes of system administration, updates, and maintenance. DIT contractors may also have access to FIVE in order to administer and maintain associated network resources.

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

[4] The TSP software/architecture stores the documents and information required. Sometimes the data is stored on-site at the institution utilizing the TSP's software; other times the data is stored at the TSP-owned Data Center.

Access to FIVE is granted based on examination staff by region. Only examiners in a given region can access files in that region. Regional access is granted through regional Active Directory groups. Membership in the Active Directory group must be requested via the FDIC's access management system [Access Request and Certification System (ARCS)] and approved by their Manager/Supervisor. 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.

4.3 Do other systems (internal or external) receive data or have access to the data in the system? If yes, explain.

☐ No

☒ Yes Explain: A user can manually attach/upload loan image files to Examination Tool Suite (ETS)[5] linesheets in order to support examination conclusions and for retention purposes. A linesheet is pre-populated in ETS with loan data provided by the bank. Examiners use the linesheet to document findings of loan review (financial analyses, collateral reviews, violations, technical exceptions, and reasons for classification, etc.).

4.4 If other agencies or entities use data in the system, explain the purpose for sharing the data and what other policies, procedures, controls, and/or sharing agreements are in place for protecting the shared data.

No other agency or entity has access to the system.

4.5 Who is responsible for assuring proper use of data in the system and, if applicable, for determining what data can be shared with other parties and systems? Have policies and procedures been established for this responsibility and accountability? Explain.

The FIVE Program Manager/Data Owner is responsible for the management and decision authority over a specific area of corporate data. The FIVE Program Manager/Data Owner and RMS Information Security Manager (ISM) serve as the sources of information for data definition and data protection requirements and are collectively responsible for supporting a corporate-wide view of data sharing.

Although the FIVE Program Manager/Data Owner and RMS ISM share overall responsibility for assuring proper use of the data, it is every user's responsibility to abide by FDIC data protection rules, which are outlined in the annual IT Security and Privacy Awareness Certification, that all employees take and certify that they will abide by the FDIC's Rules of Behavior for data protection. This makes it the responsibility of every user to ensure the proper use of corporate data.

4.6 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?

FDIC contractors are involved in the maintenance and support of the encrypted NetApp storage device and FIVE web servers.[6] These contractors are subject to the FDIC's contract provisions for confidentiality and non-disclosure.

Section 5.0: Data Integrity and Security

The following questions address how data security and integrity will be ensured for the system/project.

5.1 How is data in the system verified for accuracy, timeliness, and completeness?

FIVE receives imaged loan documents from FIs and TSPs, along with a supporting XML file that contains metadata about the loan documents, including a list of all documents requested for the review. FIVE uses

[5] See PIA for ETS at https://www.fdic.gov/about/privacy/documents/examination-tools-suite.pdf.

[6] Note: Images/data are stored on a net app server and viewed through the locally installed client. They are never viewed over the web.

the metadata to verify the completeness and accuracy of the files received through a programmatic/automatic process.

Note: The institution inputs the metadata when they scan or import documents into their imaging system. This metadata is passed to the FDIC in the previously explained export process. The automated validation process validates that the metadata is in the correct format and that all the documents identified in the metadata have also been uploaded.

5.2 What administrative and technical controls are in place to protect the data from unauthorized access and misuse? Explain.

Access to FIVE data is limited to specific Active Directory groups. Only RMS and DCP field examiners, the RMS FIVE administrative team, and RMS/DCP field management will have access to the data, and access is further limited by region.

All FIVE documents are stored on encrypted storage, be it on the NetApp storage device[7] or an examiner's laptop. All data is purged from both the storage device and laptop 90 days after the start of an exam, or if an extension is requested, upon completion of the extension. Extensions are granted in 30-day increments.

Note: In order to document the examination process, only pertinent documentation is moved to RADD or ETS, which are the systems of record for Workpapers and line sheets, respectively. All documents and metadata are purged from FIVE after the conclusion of the examination.

Section 6.0: Data Maintenance and Retention

The following questions address the maintenance and retention of records, the creation of reports on individuals, and whether a system of records is being created under the Privacy Act, 5 U.S.C. 522a.

6.1 How is data retrieved in the system or as part of the project? Can it be retrieved by a personal identifier, such as name, social security number, etc.? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

The FIVE application does not operate as a Privacy Act System of Records. FIVE permits FDIC examination staff to temporarily access and review a financial institution's customer loan documentation provided to FDIC for the purpose of assessing the institution's lending practices and credit quality. The loans selected by FDIC for review may be retrieved using any of the identifying information obtained from the financial institution's preexisting loan information fields. Once the Report of Examination is final, the supporting documentation is archived and the financial institution's customer loan documentation is deleted from FDIC systems. The Report of Examination and supporting documentation is indexed and retrieved by the financial institution's number and not by reference to any individual's name or other unique identifier.

6.2 What kind of reports can be produced *on individuals*? What is the purpose of these reports, and who will have access to them? How long will the reports be maintained, and how will they be disposed of?
Not applicable – no reports can be produced on individuals.

6.3 What are the retention periods of data in this system? 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.

[7] NetApp refers to a type of disk storage device which owns and controls a filesystem that presents files and directories over the network.

FIVE purges all loan image files ninety (90) days after an exam has been started, unless a request for extension has been made. If an extension is made to support an exam running longer than 90 days, all loan image files are purged 90 days after the extension date.

Loan files that are used to support examination conclusions are uploaded into ETS and are retained per the retention periods defined by the FDIC Reports and Information Management (RIM) Policy Manual 1210.1, which references the Records Retention Schedule (RRS).

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

The FIVE application does not operate as a Privacy Act System of Records.

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

Not applicable.

Section 7.0: Business Processes and Technology

The following questions address the magnitude of harm if the system/project data is inadvertently disclosed, as well as the choices the Corporation made regarding business processes and technology.

7.1 Will the system aggregate or consolidate data in order to make privacy 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?

No, the system will not aggregate or consolidate data in order to make privacy determinations or derive new data about individuals.

7.2 Is the system/project using new technologies, such as monitoring software, SmartCards, Caller-ID, biometric collection devices, personal identification verification (PIV) cards, radio frequency identification devices (RFID), virtual data rooms (VDRs), social media, etc., to collect, maintain, or track information about individuals? If so, explain how the use of this technology may affect privacy.

No, FIVE is not using any of these new technologies to collect, maintain, or track information about individuals.

7.3 Will the system/project provide the capability to monitor individuals or users? If yes, describe the data being collected. Additionally, describe the business need for the monitoring and explain how the information is protected.

FIVE does not have the capability to monitor individuals or users.

7.4 Explain the magnitude of harm to the Corporation if privacy-related data in the system/project is disclosed, intentionally or unintentionally. Would the reputation of the Corporation be affected?

The Corporation would experience significant reputational risk if any information was inappropriately accessed or obtained from the system.

7.5 Did the completion of this PIA result in changes to business processes or technology? If yes, explain.

No.