FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)

for

Legal Division (LEGAL)

Regulations and Rules (RAR) Provisional Service

Date Approved by Chief Privacy Officer (CPO)/Designee:
5/13/2015

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 Federal Deposit Insurance Corporation (FDIC) Legal Division developed the Regulations and Rules (RAR) Provisional Service as an interim solution to FDIC's Online Ordering System (OOS)[3] that is being retired. The provisional service utilizes Qualtrics to facilitate the public's ability to continue to order paper copies of FDIC Regulations and Rules on www.fdic.gov. The public can also subscribe to receive automatic updates (six per year). For Subscriptions a list is maintained to automatically ship updates (6/year).

Data elements collected through Qualtrics include: name, organization (optional), mailing address, telephone number, and email address. Names and mailing address are required to fulfill subscription requests and ship

[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.

[3] The FDIC, through several of its Divisions, provides to the public, businesses, community organizations and other federal agencies a number of products, publications and materials. The Online Ordering Solution (OOS) is a centralized, web-based system that facilitates FDIC's order and fulfillment process for these publications and materials. The OOS Privacy Impact Assessment (PIA) is available on FDIC.gov.

the paper documents ordered; telephone numbers and email addresses are collected to resolve any issues during the review of the order prior to fulfillment. Individuals that call, mail or make requests by other means will be guided to the web site to complete the online order form or allow FDIC staff to enter the information they provide. Once collected, the information will be maintained in a spreadsheet in a secured environment with access limited to authorized users.

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.

The provisional service collects the following information from members of the public who order paper copies of FDIC Regulations and Rules: Name, Organization (optional), Mailing Address, Telephone Number, and Email Address. This contact information may be personal or work-related, depending on what the individual chooses to provide.

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

The information is used for the following purposes:

- Name and Mailing Address are needed to ship the paper documents ordered.
- Telephone Number and Email Address are collected to resolve any issues during the review of the order prior to fulfillment.
- For Subscriptions, a list is maintained to automatically ship updates (6/year).

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

Members of the public enter their information into an online order form on the RAR website. Individuals that call, mail or make requests by other means will be guided to the website to complete the online order form or allow FDIC staff to enter the information they provide. Once collected, the information will be maintained by FDIC in a spreadsheet in a secured environment with access limited to authorized FDIC users.

3.4 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.

None.

3.5 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.

None.

3.6 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)?

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

If the individual does not wish to provide a Name, Mailing Address, Telephone Number, and Email Address on the website, they can email regs@fdic.gov to order the documents desired.

However, in order to fulfill order requests, individuals must provide the information required for shipping.

☐ No Explain: Not Applicable

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.

A small number of authorized FDIC personnel in the Legal Division will have access to the data in the provisional service. Currently, the following four (4) authorized users have access for the purposes described below.

1. One (1) Legal Information Technology Unit (LITU) developer to develop and maintain the web page.
2. Two (2) Executive Secretary Section (ESS) Subject Matter Experts (SMEs) to maintain the subscription list, respond to questions submitted through regs@fdic.gov, and review and forward the orders for fulfillment.
3. One (1) Executive Secretary Section (ESS) staff to fill, package, and ship the documents ordered.

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

All access granted is determined on a "need to know" basis. Guidelines established in the Corporation's Access Control policies and procedures are followed. Controls are documented in the official FDIC system documentation. In addition, the following procedures and controls are in place for granting access to data in the provisional service:

- An Identity Access Management System (IAMS) request must be submitted for access to Qualtrics, which is limited use software.
- Access to the development and maintenance of the web page is only accessible to the Legal Information Technology Unit (LITU) developer, via Qualtrics.
- The results must be sent from Qualtrics to the two Executive Secretary Section (ESS) Subject Matter Experts (SMEs) maintaining the subscription list (#2 in 4.1 above) by the Legal Information Technology Unit (LITU) developer.
- The results must be sent from the two Executive Secretary Section (ESS) Subject Matter Experts (SMEs) maintaining the subscription list to the staff fulfilling the order (#3 in 4.1 above).
- In order to access the data for this collection, access to Qualtrics and the Legal Information Technology Unit (LITU) developer's library is needed. To collect information (i.e., individual only has access to Qualtrics) access to the development server for www.fdic.gov and Remedy requestor is also needed.

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.

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.

Not Applicable. No other agencies or entities use data in the provisional service.

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 Program Manager in the FDIC Executive Secretary Section (ESS) has overall responsibility for ensuring the proper use of the data by authorized FDIC users, in accordance with FDIC privacy and security policies. The Program Manager and Legal Information Security Manager (ISM) serve as the source of information for data definition and data protection requirements and are collectively responsible for supporting a corporate-wide view of data sharing.

In addition, it is every RAR user's responsibility to assure proper use of data they access in the provisional service. All FDIC network users are required to complete the Corporation's annual Information Security and Privacy Awareness Training, which includes the Rules of Behavior to which all users must adhere. This training also states specifically the rules for protecting and preventing the compromise and misuse of sensitive information and PII.

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?

Not Applicable. Contractors are not involved with the design and maintenance of the provisional service.

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?

- The requestor is responsible for inputting correct and complete information (Order information, Name, Mailing Address, Telephone Number and Email Address).
- The web page has built in validation checks.
  - Only 10 or fewer of any one document may be ordered on www.fdic.gov. (Larger orders require emailing regs@fdic.gov)
  - A web page to permit the customer to review the accuracy of the documents ordered is provided.
  - Required fields MUST be completed (Name, Mailing Address, Telephone Number, and Email Address) or the order cannot be submitted.
  - The web page checks whether State, Zip Code, Telephone Number and Email Address have been entered on the proper format (i.e., An email address without an "@" symbol will not be accepted). If one or more of these fields are NOT in the proper format the order cannot be submitted.

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

Access levels and permission levels have been established, and access is granted only to those persons who have "a need to know" the information contained in the provisional service in order to carry out their official job duties. Authorized FDIC users will be responsible for abiding by the Rules of Behavior policies. FDIC users

will be required to follow Corporate and Division policies concerning the appropriate handling and protection of sensitive information. FDIC users also are reminded of their responsibilities during annual privacy and security awareness training.

Additionally, access requests will be controlled and tracked via the FDIC's IAMS process. All users who have access to the data must have the approval of their Manager/Supervisor and the Program Manager/Data Owner of the requested capability in order to be granted access.

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.

Data is downloaded in an Excel spreadsheet either as a .csv file or as a report. This is used to fill the orders and maintain a subscription list.

The data can be retrieved by personal identifier (Name); however, a specific order would only be looked up by Name in the event the individual contacts the FDIC regarding an issue with an order.

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?

Data is downloaded in an Excel spreadsheet either as a .csv file or as a report. This is used to fill the orders and maintain a subscription list. The subscription list is used to send out updates (future supplements) to subscribers.

Four staff have access to the reports as follows:

1. One Legal Information Technology Unit (LITU) developer to develop and maintain the web page.
2. Two Executive Secretary Section (ESS) Subject Matter Experts (SMEs) to maintain the subscription list, respond to questions submitted through regs@fdic.gov, and review and forward the orders for fulfillment.
3. One Executive Secretary Section (ESS) staff to fill, package, and ship the documents ordered.

Once the periodic report is transferred from the Legal Information Technology Unit (LITU) developer to the two Executive Secretary Section (ESS) Subject Matter Experts (SMEs) who maintain the subscription list, the data is purged from the provisional service. The data is added to and maintained in a legacy Excel spreadsheet.

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.

FDIC Records Management Policy will apply. All records will be maintained until they become inactive, at which time they will be retired or destroyed in accordance with National Archives and Records Administration (NARA) and FDIC Records Retention and Disposition Schedules. Disposal is completed by electronic purging and removal of records.

Once the periodic report is transferred from the Legal Information Technology Unit (LITU) developer to the two Executive Secretary Section (ESS) Subject Matter Experts (SMEs) that maintain the subscription list, the data is purged from the provisional service.

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

This provisional service will operate under the following FDIC Privacy Act SORN: "30-64-0031 Online Ordering Request 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 provisional service will not aggregate or consolidate data in order to make privacy determinations.

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. The provisional service is not using new technologies, such as SmartCards, RFID, PIV cards, etc., to collect 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.

No. The provisional service will not provide the capability to monitor individuals.

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 provisional service contains limited privacy-related data, consisting only of names and contact information, for purposes of filling publication/subscription order requests. This PII data is not contextually sensitive in nature and is generally publically available. Thus, exposure of the data would have a minimal adverse effect on the Corporation and affected individuals, and the risk of reputational harm to the FDIC is deemed to be Low. To minimize the risk of harm, the information will be maintained in a secured environment with access limited to authorized users with a "need to know."

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

No.