FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)

for

RMS/BADS

CEP Recruit System (CEPRecruit)

Date Approved by Chief Privacy Officer (CPO)/Designee:
9/20/2016

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 CEP Recruiting System (CEPRECRUIT) is a web-based application built using the Oracle Application Express tool. The system was created and is owned by the Division of Risk Management Supervision (RMS) Business Analysis and Decision Support (BADS) section in Washington.

The application is used to query applicant and vacancy data in the Reporting Data Mart Migration (RDMM) database and to output rosters of applicants for CEP recruiting events to Microsoft Excel. The application is accessible only to the RMS BADS developers and Administrative Management Section (AMS) staff responsible for CEP hiring activities, which currently amounts to about 5 users. To access the application, a member of the BADS staff must enter the user's NT ID into an internal table. Prior to a CEP recruiting event (which

[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.

typically takes place 2-3 times per year), BADS or AMS staff will log into the application, search for the vacancy announcement code, generate a list of applicants, and export this data to Excel.

The spreadsheet is then updated with information captured during the CEP recruiting event: applicant's full name, home address, phone number (non-work), employee ID number (EIN), email address (non-work) and military status or records (to indicate veteran's preference). Functionality to capture additional information regarding the applicant's performance during the event and the ultimate selection decision is not presently used. This data can be uploaded to the database if desired by the AMS staff.

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. Applicant's full name, home address, phone number (non-work), email address (non-work), EIN, and military status or records.

3.2 What is the purpose and intended use of the information you described above in Question 3.1? To have the most up-to-date applicant information at the ready for prospective permanent hires at the FDIC.

3.3 Who/what are the sources of the information in the system? How are they derived? Individuals directly provide their information at CEP recruiting events.

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? No Federal, state, and/or local agencies provide data for use in CEPRECRUIT.

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. No other third-party sources provide data to CEPRECRUIT.

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)?

☐ 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: Once individuals provide their information to a recruiter, they do not have the opportunity to opt out.

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. Data is prepared by the RMS BADS developers and used by the AMS staff responsible for CEP hiring activities.

4.2 How is access to the data determined and by whom? Explain the criteria, procedures, controls, and responsibilities for granting access. The RMS BADs group grants access to specific NT IDs.

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.** No other agencies or entities use data in CEPRECRUIT.

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 RMS BADS group Program Manager is responsible for making sure the proper people have access.

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?** No contractors are involved with the design or maintenance of CEPRECRUIT.

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? Data is self-reported by individuals, which is generally considered the preferred method of collecting information to ensure accuracy, timeliness, and completeness. CEPRECRUIT relies on individuals to provide accurate information on themselves.

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

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. Yes, data is retrieved by personal identifier. Data is retrieved within CEPRECRUIT by name of applicant.

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? Reports are produced of job vacancies and which applicants have applied for those vacancies. Reports can be searched by applicant's name, and from there the user may view the rest of the applicant's information specified in question 3.1. Reports are produced by authorized users of CEPRECRUIT and distributed to administrative staff for hiring purposes.

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. The retention periods of data/records are covered by FDIC Records Retention Schedules. Data is retired and destroyed in accordance with National Archives and Records Administration (NARA) guidance and FDIC Records Disposition Schedules.

6.4 In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this system operate? Provide number and name. This system operates under the following FDIC Privacy Act System of Records Notice (SORN): "30-64-0011, *Corporate Applicant Recruiting, Evaluating, and Electronic Referral Records*."

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

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. The system only generates a roster based on a job announcement so the FDIC can contact applicants for a possible job opportunity.

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. N/A

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. N/A

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 reputation of the Corporation should not be affected, as CEPRECRUIT only shows which applicants have applied for specific job vacancies. The magnitude of harm to the Corporation would be very low.

7.5 Did the completion of this PIA result in changes to business processes or technology? If yes, explain. No.