FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

# Privacy Impact Assessment (PIA)

for

## Division of Risk Management Supervision (RMS)

## Background Investigation Database System (BIDS)


Date Approved by Chief Privacy Officer (CPO)/Designee*
1/26/2018

# 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 FDIC's Background Investigation Database System (BIDS) is used for conducting background investigations (BIs) in connection with applications and notices submitted to the FDIC, such as applications for Federal Deposit Insurance (FDI), Notices of Acquisition of Control, applications subject to Section 19 of the FDI Act, and notices subject to Section 32 of the FDI Act. BIDS provides Regional Offices and Headquarters with a nationwide, real-time, automated management tool to track and process all background investigations. The FDIC's Division of Risk Management Supervision (RMS) Cyber Fraud and Financial Crimes (CFFC) Section is responsible for conducting these background investigations on individuals in conjunction with federal agencies including, but not limited to, the Federal Bureau of Investigations (FBI), Drug Enforcement Administration (DEA), and Immigration and Customs Enforcement (ICE).

[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.

BIDS tracks and manages BI requests (e.g. FBI Fingerprint Checks, FBI Name Checks, and Financial History Checks) for investigations of potential bank directors, officers, and principals (subjects of investigations). These data requests contain Social Security numbers (SSNs) and other sensitive personally identifiable information (PII) about the subjects being investigated.. Accordingly, BIDS secures the data according to FDIC policy, ensuring that the data is maintained in a secured, networked environment that can be accessed only by authorized RMS personnel at Regional and Washington Office locations. Critical features of the system include:

1. Data is accessible nationwide within the FDIC (Regional Offices and Headquarters)
2. Data is stored in a secure database environment
3. An applicant's BI case is tracked through the entire life cycle
4. BI request documents are auto-generated (PDF)
5. Notifications to certain users are automated at key event points
6. Legacy (converted) BI data is presented
7. Capability to generate various management reports, such as Monthly, Quarterly, and Annual Volume Reports

BIDS is composed of a secure web front-end to capture and manage BI case data. The front-end interfaces with a secure and robust database system that has the ability to both track BIDS application activities and also provides an audit capability.

## 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.**

BIDS contains the following personal information about potential bank directors or officers (BI subjects): Name, Maiden/Alias Name, SSN, Passport Number, Date of Birth, Home and Business Address, Mother's Maiden Name, Father's Name, Employment Status/Records, Investigative Reports/Data, Legal Documents/Records/Notes, Date/Place of Prior Convictions, and Name(s)/Address(es) of business(es) with which the BI subject is associated. BIDS also contains the results of BIs (Name Checks, Fingerprint Checks, Credit Checks) conducted on the subjects. Reports on BI results may be attached, and associated comments may be input.

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

BIDS is used for conducting BIs in connection with applications and notices submitted to the FDIC, such as applications for Federal Deposit Insurance (FDI), Notices of Acquisition of Control, applications subject to Section 19 of the FDI Act, and notices subject to Section 32 of the FDI Act. Refer to Section 3.3 for additional information.

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

**a) Explain the business purpose requiring the collection of SSNs.**

The FDIC is responsible for conducting background checks in connection with applications and notices submitted to the FDIC, such as applications for Federal Deposit Insurance (FDI), notices of acquisition of control, applications subject to Section 19 of the FDI Act, and notices subject to Section 32 of the FDI Act. The SSN is specifically needed to perform these required BIs in order to obtain records about the applicants from federal law enforcement agencies and consumer finance authorities.

**b) Provide the legal authority which permits the collection of SSNs.**

**Other - give justification:**
The FDIC in considering approval of Federal Deposit Insurance Applications is required by Section 5(ad) of the Federal Deposit Insurance Act (FDI Act) (12 U.S.C. 1815(a)(4) to consider certain statutory factors under Section 6 of the FDI Act (12 U.S.C. 1816), including the general character and fitness of management of the institution, its capital adequacy, and risk to the Deposit Insurance Fund. The FDIC is also required to conduct, investigate, and independently verify the accuracy and completeness of information submitted by persons named in Change in Control Notices under Section 7(j) of the FDI Act (12 U.S.C. 1817(j)). The FDIC uses background investigation information as part of its evaluation of the competence, experience, integrity, and financial ability of individuals involved in the organization, management, or control of institutions for which a Federal Deposit Insurance Application is submitted, or each person named in a Change in Control Notice.

Under Section 19 of the FDI Act (12 U.S.C. 1829), any person convicted of any criminal offense involving dishonesty, breach of trust , or money laundering, or has agreed to enter into a pretrial diversion or similar program in connection with the prosecution of such offense, may not become an institution-affiliated-party of an insured depository institution; own or control, directly or indirectly, any insured depository institution; or otherwise participate, directly or indirectly, in the conduct of the affairs of any insured depository institution without the prior written consent of the FDIC. The FDIC uses background investigation information in connection with applications subject to Section 19.

Section 32 of the FDI Act (12 U.S. C. 1831i) also requires an insured depository institution to notify the FDIC of the proposed addition of an individual to an insured state bank or state savings association's board of directors or senior management at least 30 days before such addition if the insured state bank or state savings association fails to meet minimum capital requirements; is troubled; or the FDIC determines, in connection with its review of a capital restoration plan required under Section 38 of the FDI Act (12 U.S.C. 1831o) or otherwise that such prior notice is appropriate. The FDIC is required to disapprove a Section 32 Notice if the FDIC determines that the competence, experience, character, or integrity of the individual involved indicates that it would not be in the best interest of the depositors of the institution or public if the individual is permitted to be employed by, or associated with, the insured state bank or state savings association. The FDIC also uses background investigation information to determine whether grounds exist for a Section 32 Notice to be disapproved.

Sections 5, 6, 7(j), 19, and 32 of the FDI Act require FDIC action as stated above and background investigation information is essential to the performance of the FDIC's statutory responsibilities. This information is also covered by Part 309 of the FDIC's regulations (12 C.F.R. Part 309), which safeguard confidential information. For all background investigations conducted by the FDIC, the subject signs a consent for the background investigation to be performed as part of the Federal Deposit Insurance Application, Notice of Acquisition of Control, Section 19 Application, and Section 32 Notice.

**c) Identify whether the SSN is masked or otherwise truncated within the system:**
SSNs are not masked or truncated within the system, as FDIC staff needs the ability to search, verify, and validate an individual's identity.

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

The individual undergoing the BI (BI subject) provides the personal information specified in Section 3.1 when he/she completes and submits to FDIC an 'Interagency Biographical and Financial Report' (OMB No. 3064-0006); or, the individual may provide that information in a packet prepared and submitted to FDIC using OMB Form No. 3064-0006 as a guideline. Once FDIC receives the information from the individual in hard copy (typically via FedEx/UPS), an authorized RMS user manually enters the information into BIDS and scans and uploads any applicable forms as attachments to the case (hard copies are maintained in a locked file room; separate electronic copies, when received, are not maintained). If information is missing, the FDIC Case Manager may contact the individual to obtain it. Additionally, authorized BIDS users will add data for tracking the requests, as well as the results of each BI processed (Fingerprint, Name Checks, or FDIC DOA Library Requests, such as credit checks). Upon receipt of information from the

agencies providing BI information, the Case Manager may enter appropriate notations into the freeform text field on the relevant "Edit BI Status" screen.

BIDS pulls data from Structure Information Management System (SIMS) (lists of countries and states). BIDS also pulls from the Corporate Reference Database (CRD) the list of business addresses and phone numbers of FDIC Supervisory Areas. Additionally, BIDS queries the Formal and Informal Action Tracking (FIAT) database (part of Virtual Supervisory Information on the Net [ViSION]) and pulls matching records (the record ID and address) for people matching a BIDS individual's first name and last name.

BIDS relies on the Active Directory (AD) to authenticate a BIDS user's login and password, upon a login request. Additionally, BIDS uses the AD to pull the list of approvers and Case Managers from the BIDS AD Groups. For each one of these users, BIDS retrieves the full name and office phone number.

**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.**

FDIC relies on the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), and the Immigration and Customs Enforcement Agency (ICE), to provide Name Checks and Fingerprint Check results for BI subjects. The results of these Name Checks and Fingerprint Checks are recorded in the system by authorized users. FDIC Form 6700/01 (Name Check Form) is used to facilitate a Name Check request, whereby the form is forwarded to the respective agencies via secure email, fax, or FedEx/UPS (overnight express), completed by the agencies, and subsequently returned to FDIC via secure email, fax, or FedEx/UPS (overnight express). The FBI processes Fingerprint Checks for the FDIC. The information obtained from conducting the Name Checks and Fingerprint Checks will be used to evaluate the suitability of potential bank directors, officers, and principals. The results of these Name Checks and Fingerprint Checks will be recorded in the system by authorized FDIC users. However, these federal agencies will not have direct access to BIDS.

State and/or local agencies do not provide data for and do not have access to this 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.**

Through the FDIC Library, different types of background checks will be requested using the BIDS system. BIDS will automatically generate pre-filled Information Request Forms for processing by the FDIC DOA Library Staff. Additionally, an email will be generated by BIDS to a controlled-access mailbox (limited to Library staff members) containing a link to the Information Request Form(s). A Library Staff member will be responsible for logging into BIDS, viewing and processing the Information Request Form(s) and posting the associated BI information in BIDS. FDIC Form 3020/03B (Consumer Credit Report Request), and FDIC Form 3020/11 (Library Publications Order Form) are generated by BIDS and used to facilitate these requests.

For example, there are consumer Credit Checks (via Equifax, Experian or Trans Union) and Dun and Bradstreet / Experian for business and commercial identity checks. BIDS will also be used to request checks on businesses associated with individuals undergoing a BI; for example Fitch, Moody's, Standard's & Poor's (S&P), and LexisNexis. The requests described above are originated and tracked within BIDS and BIDS stores the data collected via these checks. Any hardcopy documentation collected in conjunction with these requests will be maintained in accordance with FDIC policies.

**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)?**

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

☒ No Explain: Individuals cannot "opt out" of providing their personal information or consent to only particular use (e.g., allowing basic use of their personal information, but not sharing with other government agencies) because all PII requested is required and necessary to conduct a full comprehensive background investigation. In addition, this information must be shared with other government agencies in order to complete aspects of the background check which are done solely within those agencies (i.e., FBI fingerprint checks). In the event an individual refuses to provide the requested information necessary for conducting a background check, their approval to be a bank director or officer will be denied.

## 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.**

Appropriate RMS Regional and Headquarters staff are granted access to BIDS. RMS Assistant Regional Directors (ARDs) are responsible for coordinating Regional Office access to BIDS in accordance with appropriate security policies and procedures. ARDs can approve additional users of BIDS based on their job requirements and in accordance with the security requirements of BIDS.

The purpose for user access supports the Corporation's responsibilities and procedures for conducting background investigations in connection with applications and notices submitted to the FDIC, such as applications for Federal Deposit Insurance (FDI), notices of acquisition of control, applications subject to Section 19 of the FDI Act, and notices subject to Section 32 of the FDI Act.

BIDS User Categories for Access Control

- Regional Director
- Area Director
- Deputy Regional Director
- Assistant Regional Director
- Case Manager
- Risk Management and Applications Section Staff
- FDIC Library Reference Services Section Staff
- READ-Only User
- REGULAR User
- Washington User
- FDIC Library User
- Approver
- Administrator

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

RMS Assistant Regional Directors (ARDs) will be responsible for managing who has access to BIDS in their regions and need to manage that access in accordance with current FDIC Security Policies and Procedures and the knowledge that BIDS contains the highest level of PII and requires the highest level of security possible within the FDIC.

Access to BIDS is facilitated, tracked, and managed using the Corporation's Access Request and Certification System (ARCS), formerly known as Identity Access Management System (IAMS).

Management approval is required for access to the BIDS application, which is role-based according to job function, and contingent on a business need to know. Those individuals identified in the response to

Question 4.1 under the heading of "BIDS User Categories for Access Control" will be notified upon beginning their position that among their responsibilities will be to submit a request through Access Control or a request may be submitted upon their behalf for BIDS access. Other individuals may obtain access to BIDS by submitting an Access Control request, based on their job responsibility to conduct background investigations of potential bank directors and/or officers.

Additionally, the hardcopy documentation (for instance, reports associated with requests made via FDIC Form 3020/03B [Consumer Credit Report Request] and FDIC Form 3020/11 [Library Publications Order Form] are generated by BIDS and used to facilitate these requests) obtained and maintained in conjunction with the BIDS application is maintained in accordance with FDIC policies.

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

☒ No
☐ Yes There are NO internal or external systems that receive or have access to BIDS data

**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 will have direct access to the data in BIDS. BIDS will, however, produce the Name Check forms (FDIC Form 6700/01) that are printed by BIDS users in the Washington Office and delivered via secure email, faxed, or delivered via FedEX/UPS (overnight express) to agencies that conduct Name Checks (DEA and ICE). The information requested using FDIC Form 6700/01 is subsequently returned by the pertinent agency to FDIC via secure email, fax, or is delivered via FedEx/UPS (overnight express). The Name Check Form includes the following personal data elements: Name, Social Security Number, Date of Birth, Maiden/Alias Name, Home Address, Employment History, Date and Place of Prior Convictions, Father's Name, Mother's Maiden Name, Passport Number. DOA has an established set of contractual agreements with Financial/Credit Check agencies. The FBI processes Name Checks and Fingerprint Checks for the FDIC.

**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**.

FDIC Division of Information Technology (DIT) is responsible for ensuring that sufficient safeguards and controls are in place to avoid the unauthorized or unintended release of personal data, while individual BIDS users are responsible and accountable for assuring the proper collection and use of the data, and that the sharing of any BIDS information with outside agencies is appropriate. (DIT is responsible for ensuring that the ARCS application, which prospective users will use to enter access requests, accurately processes these requests, and for the provisioning of Active Directory groups accordingly.) The FDIC DIT Program Manager has overall responsibility for the BIDS application and is accountable for establishing the criteria, procedures, controls, and responsibilities to prevent a compromise of the integrity of the data being collected.

DIT is responsible for ensuring that the data used in the development (DEV) and quality assurance (QA) environments has been "sanitized" to remove all actual PII in converted records. DIT controls the DEV environment and data.

DIT and RMS jointly control the QA environment and data, and RMS controls the data in the PRODUCTION environment. The data in the Oracle Database (DBMS) and the advanced engine management (AEM) environment are under the control of DIT DBAs. DIT is also responsible for ensuring that the data in any of these three environments is secured and not accessible in any way to unauthorized users.

DIT is responsible for securing the communication channel between the BIDS end user (desktop/laptop) and the BIDS application server(s).

**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?**

Contractors have been the main source for design and construction tasks. Yes, a Contractor Confidentiality Agreement/Non-Disclosure Agreement has been signed. A contractor will support the maintenance of the system but will not have access to the production environment.

## 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 will be checked for completeness by visual inspection by authorized BIDS users. Then data will be manually entered into the BIDS system. The BIDS system will alert the user if certain required information is missing.

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

Data from outside the FDIC is collected for conducting background checks in connection with applications and notices submitted to the FDIC, such as applications for Federal Deposit Insurance (FDI), notices of acquisition of control, applications subject to Section 19 of the FDI Act, and notices subject to Section 32 of the FDI Act. Results are delivered via secure email, fax, or FedEx/UPS (overnight express). The hard copy data is verified by the authorized RMS user who has access to BIDS. BIDS users will check the authenticity of the source of the incoming mail and its contents.

## 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 may be retrieved only by authorized personal who have logged into BIDS. The data can be retrieved using a personal identifier like SSN and Name. There are numerous other retrieval options, but they do not include the use of personal identifiers.

**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?**

BIDS will produce five reports. Four of these reports are Management Reports which present aggregate/counts only, and do not show any PII; these reports are presented in an Excel format. The fifth report is called the "Background Investigation Summary Report (Individual Information)". It displays the status information for the BI Case, including the associated Individuals' names and SSNs; this report is presented in PDF format. All reports will be accessible through the BIDS application. All BIDS users will have the capability of running/viewing all reports within the application – and to save them or print them.

BIDS will also produce PDF documents that are then mailed to other federal government agencies.

**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.**

Data/records maintained within BIDS are covered by the FDIC Records Retention Schedule. RMS has requested a modification of the retention requirement to properly support business needs. The system is in the process of being scheduled, and a new retention and disposition requirement of 30 years is being developed in accordance with FDIC Records Retention Scheduling procedures.

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

BIDS operates under FDIC System of Record Notice 30–64–0002, *Financial Institution Investigative and Enforcement Records* (80 FR 66984).

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

No.

## 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?**

In accordance with Federal law and policy, the BIDS system has controls in place to prevent the misuse of the data by those having access to the data. Such security measures and controls consist of: passwords, user identification, IP addresses, database permissions, and software controls. All RMS employees must meet the requirements for securing Privacy Act protected information. Additionally, BIDS users are required to complete FDIC's Corporate Information Security Awareness Training and Privacy Act Awareness Orientation on an annual basis. All users of BIDS are Corporation Employees and are required to comply with Corporate and BIDS procedures related to information security and privacy act security.

All BIDS users have a password and ID that is issued by the Corporation - and must be assigned to the appropriate BIDS security groups/roles.

Additionally, the system will record the user's id and access time(s) when BI Case data is accessed.

**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 system is not using monitoring software, SmartCards, Caller-ID, RFID, social media, or other similar new technologies to 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.**

There is no user monitoring.

**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?**

Yes, the reputation of the Corporation could be affected. The magnitude of harm would depend on the specific data, the number of records disclosed, and the use of the improperly disclosed data. Business partners and submitters of PII information would be contacted per FDIC data breach procedures.

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

No