FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

# Privacy Impact Assessment (PIA)
# for
# FDIC Board of Directors Operations


March 30, 2022

# 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's public-facing website, which describes FDIC's activities that impact privacy, the authority for collecting personally identifiable information (PII), and the procedures to access and have PII amended or corrected if necessary.

# SYSTEM OVERVIEW

Describe what this information system[1] does in terms of purpose, functionality, and PII collection/use. What is the goal of the system? What gap does it serve to close?

**Abstract**

The FDIC Executive Secretary serves as secretary to the Corporation's Board of Directors and standing and special committees established by the Board, Committee Management Officer for all FDIC advisory committees, the Corporation's Federal Register officer and is an Agent for Service of Process[2] in Washington, DC. The Board designated the Executive Secretary as FDIC Administrative Officer for administrative enforcement actions[3] and in this role serves as FDIC Docket Clerk. In executing these responsibilities, the Executive Secretary leverages several different systems and platforms, collectively referred to herein as the Board of Directors Operations Tool Suite (BODOTS). The Executive Secretary uses BODOTS to index and maintain Board records, some of which include personally identifiable information (PII). The FDIC is conducting this Privacy Impact Assessment (PIA) to provide transparency to the public and to assess and mitigate any risks associated with FDIC's collection, use and maintenance of this PII.

**Background**

The Federal Deposit Insurance Corporation (FDIC) is an independent agency of the U.S. government charged with maintaining stability and public confidence in the nation's financial system by insuring deposits, examining and supervising financial institutions, making large and complex financial institutions resolvable, and managing receiverships.

The FDIC Board of Directors (Board) has had a secretary since its inception in 1933. The Deputy Executive Secretary serves as secretary to the Board and all standing and special committees established by the Board. The Executive Secretary Section (ESS) within the FDIC's Legal Division, led by the Deputy Executive Secretary, provides essential legal and logistical support to the FDIC Board, its standing and special committees. ESS plans Board and standing and special committee meetings and ensures that these Board and committee deliberations and decisions are accurately recorded. ESS maintains the official records of all Board actions from 1933 to present in the FDIC Board Records (BODREC) repository, together with certain records of Board committees and certain documents relating to actions of the Board of the Resolution Trust Corporation.

The Deputy Executive Secretary and others in ESS serve as the FDIC's *Federal Register* liaison, certifying, and authenticating officers and alternates. ESS maintains records of public comments on FDIC *Federal Register* publications.

The Deputy Executive Secretary serves as the Committee Management Officer for the FDIC's advisory committees. In this role, the ESS Operations Unit oversees administration of the FDIC advisory committees to

[1] OMB Circular No. A-130, "Managing Information as a Strategic Resource," (July 27, 2016). The Circular defines an information system as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
[2] www.fdic.gov/contact/agents-for-service-of-process
[3] www.fdic.gov/regulations/examinations/enforcement-actions/index.html

ensure compliance with the Federal Advisory Committee Act[4] and implementing regulations. This includes an annual comprehensive review of each committee that is submitted to the General Services Administration federal advisory Committee Management Secretariat.

The Deputy Executive Secretary serves as an Agent for Service of Process[5] for FDIC Headquarters in Washington, DC. (Service of process refers to the procedure employed by parties in a lawsuit to formally deliver papers/notice of legal action to the other parties and the court.) In this role, ESS maintains a log of all process served on the Executive Secretary in Headquarters.

The Board of Directors designated the Deputy Executive Secretary as the FDIC's Administrative Officer for all administrative enforcement actions, and in this capacity serves as the Docket Clerk for the Board for such actions. These include terminations of deposit insurance, cease and desist orders, removal proceedings and civil money penalties. ESS Operations manages the legal documents filed with the Administrative Officer in connection with specialized administrative proceedings pursuant to sections 7, 8, 10(c), and 19 of the FDI Act,[6] and matters pursuant to sections 10, 32, and 38 of the FDI Act. The ESS Operations Unit also prepares the record of enforcement proceedings for submission to the Board for review and final decision, and prepares the record for review if the Board's decision is appealed to a federal court. The Administrative Officer (or designee) issues certain procedural rulings during administrative enforcement proceedings (such as an extension of time), issues orders terminating the insured status of depository institutions, and serves legal papers in contested enforcement actions. For additional information about the FDIC's enforcement process and associated privacy risks, refer to FDIC's Privacy Impact Assessment for Virtual Supervisory Information on the Net (ViSION) available on FDIC's Privacy Program website.[7]

As Administrative Officer, ESS Operations Unit coordinates with the Office of Financial Institution Adjudication (OFIA) in docketing FDIC administrative actions and providing certified documents for federal courts and others. OFIA is an inter-agency group of administrative law judges (ALJs), established pursuant to the Financial Institutions Reform, Recovery, and Enforcement Act (FIRREA),[8] that presides over administrative enforcement proceedings brought by the FDIC and other Federal financial regulatory agencies, and issues recommended decisions to the relevant agency head.

**Overview and Components of Board of Directors Operations Tool Suite:**

To effectively manage its responsibilities as the Board's docket clerk, secretary and records custodian, ESS utilizes the following solutions for the purposes outlined below. These solutions are collectively referred to as the Board of Directors Operations Tool Suite (BODOTS) for purposes of this PIA.

**The Board of Directors' Records System (BODREC)**

BODREC maintains current and legacy FDIC Board meeting minutes and supporting documents. ESS previously maintained a portion of these materials in FDIC's Board Meeting Minutes (BODMIN) tracking system and Consolidated Document Information System-Board of Directors Minutes and Cases (CDIS-SUPER). BODREC replaced these legacy systems (BODMIN and CDIS-SUPER), and provides ESS with a consolidated repository for storing and retrieving documents from Board of Directors meetings within FDIC's enterprise content management solution. This enterprise solution provides a unified content management system with tools for working with many types of content (i.e. documents, drawings, scanned images, and hard copies) in a single repository for all Board meeting and notational vote action records.

Within the Legal Division, ESS has access to BODREC to store Board of Director meeting minutes and documents relevant to Board meetings; and search for relevant information from Board meetings at the request of the Board or other FDIC personnel.

**BODREC Data**

The BODREC solution maintains FDIC Board meeting minutes and supporting documents dating back to the 1930s. Some of the documents uploaded to BODREC may contain agency sensitive information

[4] The Federal Advisory Committee Act (FACA), Pub. L. 92-463, Sec. 1, Oct. 6, 1972, 86 Stat. 770.
[5] www.fdic.gov/contact/agents-for-service-of-process
[6] The Federal Deposit Insurance Act of 1950 (FDI Act), Pub. L. 81–797, 64 Stat. 873 (September 21, 1950).
[7] www.fdic.gov/policies/privacy/assessments.html
[8] Financial Institutions Reform, Recovery and Enforcement Act (FIRREA), Pub. L. 101-73, 103 Stat. 183 (1989).

or PII related to, for example, administrative enforcement or personnel actions taken by the FDIC Board of Directors, standing committees or delegated officials. The PII in these records may pertain to different categories of individuals, such as FDIC employees who are the subjects of reports or recommendations to the Board and members of the public, such as bank officers, directors or other institution-affiliated parties who are the subjects of Board matters. The type of PII varies according to the nature of a particular Board matter and could potentially include any PII collected as part of fulfilling FDIC's mission.

BODREC does not collect information directly from individuals or have any direct interconnections with other systems or government agencies. All information is manually entered or uploaded into BODREC by authorized FDIC users within the Legal Division. While BODREC does not directly receive data from other systems or agencies, certain supporting documents in BODREC could be derived or obtained from other government agencies, such as an order appointing the FDIC as receiver of a failed financial institution issued by a state court or state or other federal agency.

**FDIC Board Communication, Collaboration and Document Management Solutions**

As dictated by business need related to FDIC Board operations, ESS uses FDIC-authorized document management repositories and online communication and collaboration tools to, for example, store and share Board documents, collaborate with stakeholders, and provide streamlined stakeholder interactions. These online communication and collaboration tools simplify and replace ESS's manual business processes associated with preparing, collecting and disseminating documents in support of Board matters. These manual processes involve collecting and exchanging Board documents with FDIC and ex officio Board members and their staff primarily via secure email, scanning of hard copy documents, and hand-delivery of hard copy documents. Ex officio Board members and their staff who have access to these tools and FDIC Board materials include those principally employed by the Office of the Comptroller of the Currency (OCC) and the Consumer Financial Protection Bureau (CFPB). The Federal Deposit Insurance Act (FDI Act)[9] outlines the statutory requirements for the composition of the FDIC Board and provides the authority for collecting and sharing information related to Board matters and meetings.

**Communication, Collaboration and Document Management Solution Data**

Data maintained by ESS within FDIC-approved document repositories includes agency sensitive information and PII, such as legal pleadings obtained by FDIC agents for service of process[10] and other information collected under Board authority. Depending on the nature and scope of these pleadings, they have the potential to contain any manner of PII, including but not limited to names, contact information, Social Security numbers, fingerprints (on rare occasions), financial, criminal, employment, and investigative information, and/or other information related to the lawsuit.

Data shared with other Board members via FDIC's online communication and collaboration platform includes FDIC Board briefing packages and other documents related to FDIC Board meetings and matters. The type of PII in these documents varies according to the context and nature of a particular Board matter. When PII is included in a Board package, it frequently relates to a potential action being taken by the FDIC or another regulatory agency against an officer or director of a financial institution. The following types of PII may potentially be contained in Board packages: name, date of birth, employment status, address, telephone number, email address, and financial, criminal and investigation information. However, Board records have the potential to include any manner of PII depending on the nature of a particular Board matter.

ESS is responsible for monitoring and maintaining the content on their respective sites/repositories within the FDIC's communication and collaboration platform, including ensuring the appropriateness of the information being collected and disseminated, as well as the retention and access to that information, in line with FDIC data protection and retention policies.

[9] The Federal Deposit Insurance Act of 1950 (FDI Act), Pub. L. 81–797, 64 Stat. 873 (September 21, 1950).
[10] www.fdic.gov/contact/agents-for-service-of-process/

**Docket-SP**

FDIC pursues administrative enforcement actions[11] against financial institutions that are supervised by the FDIC or against their institution-affiliated parties (IAPs) for violations of laws, rules, or regulations, unsafe or unsound banking practices, breaches of fiduciary duty, and violations of final orders, conditions imposed in writing or written agreements. FDIC publishes enforcement orders and notices on its website.[12] For additional information about the FDIC's enforcement process and associated privacy risks, refer to FDIC's Privacy Impact Assessment for Virtual Supervisory Information on the Net (ViSION) available on FDIC's Privacy Program website.[13]

As the docket clerk for the Board and FDIC's Administrative Officer in all administrative enforcement actions, ESS serves as the custodian for all Board records and maintains the official records of all enforcement actions, whether contested or stipulated. Accordingly, the Administrative Officer (or designee) is served or copied with copies of all pleadings and these pleadings are then indexed and archived.

In support of these responsibilities, ESS utilizes Docket-SP to electronically index and retrieve enforcement and personnel action records that occur by consent without direct action by the Board of Directors. ESS creates a summary index record for each action in the Docket database for electronic tracking. The actual enforcement actions and related documents were historically maintained and tracked in hard copy form and stored locally and offsite. However, Docket-SP leverages FDIC's enterprise document management solution and provides the capability to import or link documents to the enforcement action index records, thereby replacing the FDIC's legacy Docket database and manual indexing process.

**Docket-SP Data**

Docket-SP maintains an index of administrative enforcement actions and personnel actions relating to financial institutions. ESS uploads legal pleadings and other case documents and exhibits associated with the actions. Some of the records contain agency sensitive information and/or PII about individuals who have been the subject of administrative enforcement actions by the FDIC Board of Directors, its standing committees, or FDIC officials under delegated authority. Authorized staff in ESS have access to Docket-SP to manually enter information transcribed from court/case documents. PII keyed into the system by ESS is generally limited to the names of the subjects of FDIC administrative enforcement. Other PII maintained in the system is located in the pleadings and case documents uploaded to the system.

The historical information in Docket-SP was derived from the legacy Docket application. The data in the legacy Docket databases included indexes of each FDIC enforcement action and was solely collected through manual population of the data fields. Moving to the current Docket-SP platform provided greater functionality to ESS staff to track not only enforcement action index records, but also link documents to each enforcement action in the new application.

**OES Certification (OES CERT)**

OES Cert is a desktop application/tool used by the Legal Division to produce certificates of insurance for insured financial institutions. ESS manually enters the information that is to be printed on the certificate. The date of the certificate is linked to the signature pair of active FDIC officials (Chairman and Secretary). The combined information is formatted and then printed on a blank certificate. The financial institution is given the certificate which is generally active as long as the institution is open under that name. However, a new certificate is generated if/when a financial institution changes title or when the main office of the financial institution moves to a new city or state.

**OES CERT Data**

The certificates processed by the OES CERT tool contain information about the insured financial institution (e.g., institution name and location). The certificates also contain the signatures of the FDIC Chairman and Secretary.

[11] www.fdic.gov/regulations/examinations/enforcement-actions/index.html
[12] https://orders.fdic.gov/s/
[13] www.fdic.gov/policies/privacy/assessments.html

FDIC is conducting this PIA to evaluate and document the impact that the Board of Directors Operations Tool Suite (BODOTS) has on privacy. The FDIC's System of Records Notice (SORN) FDIC-003, Administrative and Personnel Action Records,[14] provides notice of the information maintained and processed in BODOTS relating to administrative enforcement and personnel actions taken by the FDIC Board of Directors, standing committees or other delegated officials. In addition, depending on the nature of a particular Board matter, it may contain information derived from other agency recordkeeping systems of records. Such systems of records generally include: FDIC-002, Financial Institution Investigative and Enforcement Records;[15] FDIC-005, Consumer Complaint and Inquiry Records;[16] FDIC-009, Safety and Security Incident Records;[17] FDIC-012, Financial Information Management Records;[18] FDIC-013, Insured Financial Institution Liquidation Records;[19] FDIC-015, Personnel Records;[20] FDIC-018, Grievance Records;[21] and FDIC-022, Freedom of Information Act and Privacy Act Request Records.[22] The context of the data being processed determines the applicable SORN. For example, Privacy Act records relating to resolution and receivership matters would be covered by the Insured Financial Institution Liquidation Records,[23] and any Privacy Act records relating to FDIC risk management and supervision matters would be covered by the Financial Institution Investigative and Enforcement Records SORN.[24] The FDIC Identity, Credential and Access Management Records SORN[25] covers any logs, audits, or other security data regarding use of FDIC information technology resources, including access to and use of the ESS tools and resources by authorized individuals.

# 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:

- Individual Participation and Transparency
- Access and Amendment
- Accountability
- Data Minimization
- Data Quality and Integrity
- Purpose and Use Limitation

**Individual Participation and Transparency**

**Privacy Risk**: The Board of Directors Records Tool Suite (BODOTS) does not collect PII directly from subjects of Board matters. Instead, authorized Legal Division staff use BODOTS to index, maintain and share records with Board members, using information that is otherwise collected or maintained by the FDIC. Therefore,

[14] FDIC SORN-003, Administrative and Personnel Action Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[15] FDIC SORN-002, Financial Institution Investigative and Enforcement Records, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/policies/privacy/sorns.html.
[16] FDIC SORN-005, Consumer Complaint and Inquiry Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[17] FDIC SORN-009, Safety and Security Incident Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[18] FDIC SORN-012, Financial Information Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[19] FDIC SORN-013, Insured Financial Institution Liquidation Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[20] FDIC SORN-015, Personnel Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[21] FDIC SORN-018, Grievance Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[22] FDIC SORN-022, Freedom of Information Act and Privacy Act Request Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[23] FDIC SORN-013, Insured Financial Institution Liquidation Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[24] FDIC SORN-002, Financial Institution Investigative and Enforcement Records, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/policies/privacy/sorns.html.
[25] FDIC SORN-035, FDIC Identity, Credential and Access Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.

there is a risk that individuals are not aware that their PII is maintained within BODOTS and are not provided with an opportunity to directly consent or opt out prior to the collection and use of their PII within BODOTS.

**Mitigation**: This PIA and the associated SORNs detailed above provide transparency to the public regarding the collection and use of information in BODOTS. In addition, FDIC provides notice to individuals at the original point of data collection wherever possible. Specifically, in cases where Board records include PII derived from other FDIC Privacy Act systems of records (SORs), the FDIC provides notice to individuals at the original point of collection through the respective SORNs and Privacy Act Statements (PAS) for those source systems. For information that is originally collected pursuant to an administrative action or request from the FDIC, notice is provided as part of the request (e.g., in a letter request, or in the document outlining the compulsory process request). In cases where BODOTS derives PII from government agencies or other third parties, those entities are responsible for providing any applicable, required notices to the individuals from whom they initially collected the information. When FDIC collects information pursuant to court order or as part of an ongoing investigation, individuals may not receive notice (or the opportunity to consent) as to how their information will be used or disclosed. The use and disclosure of this information is governed by applicable federal law, discovery rules and court orders. When notice and/or consent opportunities cannot be provided or are not required, the FDIC provides constructive notice through its general Privacy Policy and PIAs, including this one.

**Access and Amendment**

**Privacy Risk**: Individuals who are subjects of FDIC Board matters may not be able to correct or amend inaccurate information about themselves.

**Mitigation**: Individuals may request access and amendment to their personal information in accordance with the Privacy Act and the FDIC's Privacy Act regulations, at 12 C.F.R. § 310.3 and 310.4. However, some FDIC Board records may be exempt from access under the Privacy Act or FOIA in order to prevent harm to the investigative or enforcement process. Providing individual access to such records may reveal investigative or enforcement interests on the part of FDIC. Access to records could also permit the individual who is the subject of a record to impede the Board's deliberation or FDIC's investigation and/or tamper with witnesses or evidence. In cases where BODOTS derives data from government agencies or other third-party entities, individuals should contact the source entities and agencies that originated their data to access and amend their information.

**Accountability**

**Privacy Risk**: Data maintained within BODOTS may include sensitive information about individuals involved in Board matters that presents a risk if that information is misused or used for unauthorized purposes. Inadvertent or malicious actions taken on a particular Board matter may not be traceable back to an individual.

**Mitigation**: To mitigate this risk, BODOTS employs role-based permissions to restrict access to BODOTS and the data contained therein to only authorized FDIC personnel who have a "need-to-know" in order to fulfill their job responsibilities. In addition, all users are subject and must adhere to agency policies and procedures for using, sharing and safeguarding PII. All users receive annual Information Security and Privacy Awareness training, as well as specialized training, as applicable, which helps ensure PII is handled and safeguarded appropriately. BODOTS implements auditing controls whereby actions taken by a user on a particular matter are tracked. This auditing feature maintains accountability of an action taken by an authorized user.

**Data Minimization**

**Privacy Risk**: There is a risk that Board records stored in the BODOTS could be duplicative of information in source systems and could be retained for longer than necessary to accomplish the purpose for which the information was originally collected.

**Mitigation**: FDIC maintains and disposes of the records in the Board of Directors' Operations Tool Suite according to the records schedules and policies discussed in Section 6. Within the tool suite, BODREC serves as the authoritative recordkeeping system for Board matters, and Docket-SP as the authoritative indexing system for administrative action records. ESS uploads only the minimum amount of information necessary to

accurately index action records, record Board determinations, and execute other Board operations. Any copies of BODREC data maintained on the FDIC's communication and collaboration tool must be deleted when no longer needed for reference. The FDIC's communication and collaboration tool has built-in retention schedules that can be implemented to notify users when documents have reached expiration and to automatically delete or allow users to manually delete documents when no longer needed. ESS plans to work with the Division of Administration (DOA) Records and Information Management Unit (RIMU) to determine appropriate retention and disposition procedures for documents maintained on the FDIC's communication and collaboration tool and will configure retention schedules within the tool accordingly.

**Data Quality and Integrity**

**Privacy Risk**: There is a potential risk associated with data quality and integrity because erroneous or inaccurate information could be manually entered or uploaded into BODOTS.

**Mitigation**: FDIC mitigates this risk by verifying the accuracy and completeness of information to the extent necessary for accurately recording, indexing and reporting on information about Board matters. This includes carefully recording and confirming key data, such as the dates, Board deliberations/determinations, names of parties involved, and supplemental materials associated with each Board meeting and matter, including those that may pertain to individuals. ESS vets the Board meeting minutes and accompanying materials with the Board and receives their final approval prior to uploading the official, signed copies into BODOTS. ESS does not manually key PII into BODOTS (with the exception of the name field in Docket-SP). Instead, the PII contained in BODOTS is generally located within the contents of files/documents that are uploaded by ESS; these documents undergo the aforementioned clearance process, in addition to any review and vetting process the originator undertakes in connection with their submission to the Board of Directors.

**Purpose and Use Limitation**

**Privacy Risk:** There is a risk that disclosures of information in BODOTS could be incompatible with the original purposes for which the information was collected.

**Mitigation**: To mitigate this risk, BODOTS restricts access to data to users with a "need-to-know" who require the information to perform their Board-related job responsibilities. Any information disclosures are initiated by authorized FDIC personnel who have a responsibility to share the information for purposes that are compatible with the purpose for which the PII was originally collected and/or that are otherwise legally authorized or required. Additionally, any information disclosures are made based on the nature of the records and, as applicable, pursuant to the routine uses and exemptions in the SORNs that cover the source records.

# Section 1.0: Information System

**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?**

BODOTS maintains FDIC Board of Directors (Board) meeting agendas, minutes and related briefing materials and documentation necessary to accurately record the discussions that take place during Board meetings. Content recorded from Board meeting discussions and supporting documentation may contain agency-sensitive information and PII, such as employee disciplinary data or information related to bank closings. Depending on the nature of a particular Board matter, this PII could include, but is not limited to: name, date of birth, contact information (address, email address, telephone number), and employment, financial, criminal or investigation information.

BODOTS also maintains an index of administrative enforcement actions and personnel actions relating to financial institutions, including copies of associated legal pleadings and other case documents and exhibits. These pleadings have the potential to contain any manner of PII, including but not limited to names, contact information, Social Security numbers, fingerprints (on rare

occasions), financial, criminal, employment, and investigative information, and/or other information related to the lawsuit.

In addition, BODOTS creates certificates of insurance for insured financial institutions. These certificates contain information about the insured financial institution (e.g., institution name and location) and signatures of the FDIC Chairman and Secretary. However, OESCert does not retain this information after the certificates are generated.

Since Board matters have the potential to include information pertaining to any matter in the scope of FDIC's mission, the PII contained in BODOTS could relate to various categories of individuals, including FDIC personnel, employees of other government agencies, or members of the public, such as bank officers, employees, customers, vendors (e.g., law firms, appraisers and accountants hired by open or closed banks), and depositors, or individuals who file complaints with or against FDIC (complainants).

Note: The following list of PII elements is not intended to be exhaustive. As explained above, the specific PII contained in BODOTS varies based on the nature of a particular Board matter.

| 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) (non-work) | ☒ | ☐ |
| Email Address (non-work) | ☒ | ☐ |
| 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: BODOTS System User Information) | ☒ | ☐ |

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

The following table provides common, potential sources of PII. This list is not intended to be exhaustive, as the specific PII contained in BODOTS varies based on the nature of a particular Board matter.

| Data Source | Description of Information Provided by Source |
|---|---|
| Manual Entry by ESS | The Executive Secretary Section (ESS) has access to BODOTS to store Board of Director meeting minutes and documents relevant to Board meetings, as well as to search for relevant information from Board meetings at the request of the Board or other executives. The Divisions/Offices originating the Board |

| | |
|---|---|
| | cases/matters are responsible for providing ESS with a copy. ESS, in turn, forwards cases to the Board members and their deputies and assistants. ESS uploads the final, signed minutes and other supplementary materials to BODOTS, after the Board reviews and approves them.<br><br>ESS also has access to BODOTS to index and archive administrative enforcement actions based on information transcribed from case documents. ESS is copied on all legal pleadings and indexes/appends them to the relevant action records within BODOTS. For contested proceedings, once the Office of Financial Institution Adjudication issues a recommended decision, ESS receives and uploads the administrative enforcement records with any transcripts and other associated case materials.<br><br>BODOTS does not collect information directly from individuals or have any direct interconnections with other systems or government agencies. All information is manually entered or uploaded by authorized system users. While BODOTS does not have any direct interconnections with other internal or external systems, certain supporting documents in BODOTS could be derived or obtained from other government agencies or third parties, such as an order appointing the FDIC as receiver of a failed financial institution issued by a court or state or other federal agency. |

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

All FDIC information systems must achieve an Authority to Operate (ATO) via the Assessment and Authorization process that aligns with the Risk Management Framework. Information systems that process Board information have been granted ATO or are in the process to achieve ATO. The ATO for each FDIC system is periodically reviewed as part of the FDIC Ongoing Authorization process.

# 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 Systems of Record Notice (SORN) does this information system or project operate? Provide number and name.**

The following SORN applies to the system or project: FDIC-003, Administrative and Personnel Action Records,[26] which covers minutes of the meetings of the FDIC Board of Directors or standing committees and orders of the Board of Directors, standing committees, or other officials as well as annotations of entries into the minutes and orders. In addition, depending on the nature of a

[26] FDIC SORN-003, Administrative and Personnel Action Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.

particular Board matter, BODOTS may include information derived from other agency recordkeeping systems of records. Such record systems generally include: FDIC-002, Financial Institution Investigative and Enforcement Records;[27] FDIC-005, Consumer Complaint and Inquiry Records;[28] FDIC-009, Safety and Security Incident Records;[29] FDIC-012, Financial Information Management Records;[30] FDIC-013, Insured Financial Institution Liquidation Records;[31] FDIC-015, Personnel Records;[32] FDIC-018, Grievance Records;[33] and FDIC-022, Freedom of Information Act and Privacy Act Request Records.[34] The context of the data determines the applicable SORN. For example, Privacy Act records relating to resolution and receivership matters would be covered by the Insured Financial Institution Liquidation Records,[35] and any Privacy Act records relating to FDIC risk management and supervision matters would be covered by the Financial Institution Investigative and Enforcement Records SORN.[36] Further, the FDIC Identity, Credential and Access Management Records SORN[37] covers any logs, audits, or other security data regarding use of FDIC information technology resources, including access to and use of ESS tools and resources by authorized individuals.

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

Not applicable. The system is not being modified at this time. Generally, the FDIC conducts reviews of its SORNs every three years or as needed.

**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.**

The FDIC ensures that its forms, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974 and FDIC Circular 1213.1 'FDIC Forms Management Program'.

BODOTS does not collect information directly from individuals who are subjects of FDIC Board matters. However, the FDIC provides notice to individuals at the original point of collection wherever practical. In cases where Board records include PII derived from other FDIC Privacy Act systems of records (SORs), the FDIC provides notice to individuals at the original point of collection through the respective SORNs and Privacy Act Statements (PAS) for those source systems. For information that is collected pursuant to a request from the FDIC, notice is provided as part of the request (e.g., in a letter request, or in the document outlining the compulsory process request). Litigants in civil cases are made aware that courts may compel FDIC to search for and produce agency records pertaining to them and their claims during the litigation process. In addition, this PIA serves as notice to the public about FDIC's collection and use of information in BODOTS.

---

[27] FDIC SORN-002, Financial Institution Investigative and Enforcement Records, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/policies/privacy/sorns.html.
[28] FDIC SORN-005, Consumer Complaint and Inquiry Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[29] FDIC SORN-009, Safety and Security Incident Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[30] FDIC SORN-012, Financial Information Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[31] FDIC SORN-013, Insured Financial Institution Liquidation Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[32] FDIC SORN-015, Personnel Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[33] FDIC SORN-018, Grievance Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[34] FDIC SORN-022, Freedom of Information Act and Privacy Act Request Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[35] FDIC SORN-013, Insured Financial Institution Liquidation Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[36] FDIC SORN-002, Financial Institution Investigative and Enforcement Records, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/policies/privacy/sorns.html.
[37] FDIC SORN-035, FDIC Identity, Credential and Access Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.

When BODOTS receives data from a government agency or other third-party entity, it is incumbent upon the source entity to provide any applicable, required notices to the individuals from whom they collected the information. Additionally, this PIA serves as notice of the information collection.

With regard to information collected from internal FDIC systems related to employee disciplinary actions, all personnel are informed that FDIC's computing systems are monitored and that personal information may be collected. Notices are provided to FDIC personnel at logon and are also conveyed in FDIC policy documents and during employee training.

**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 provides access to agency SORNs, PIAs, Privacy Policy, and contact information for the SAOP, the Privacy Program Chief, and the Privacy Program (Privacy@fdic.gov). For more information on how FDIC protects privacy, please visit www.fdic.gov/privacy.

# Privacy Risk Analysis: Related to Transparency

**Privacy Risk**: The Board of Directors Records Tool Suite (BODOTS) does not collect PII directly from the individuals about whom Board matters pertain. Instead, authorized Legal Division staff use BODOTS to index, maintain and share records with Board members, using information that is otherwise collected or maintained by the FDIC. Therefore, there is a risk that individuals are not aware that their PII is maintained within BODOTS.

**Mitigation**: This PIA and the associated SORNs detailed above provide transparency to the public regarding the collection and use of information in BODOTS. In addition, FDIC provides notice to individuals at the original point of data collection wherever possible. Specifically, in cases where Board records include PII derived from other FDIC Privacy Act systems of records (SORs), the FDIC provides notice to individuals at the original point of collection through the respective SORNs and Privacy Act Statements (PAS) for those source systems. For information that is originally collected pursuant to a request from the FDIC, notice is provided as part of the request (e.g., in a letter request, or in the document outlining the compulsory process request). In cases where BODOTS derives PII from government agencies or other third parties, those entities are responsible for providing any applicable, required notices to the individuals from whom they initially collected the information. When FDIC collects information pursuant to a court order or as part of an ongoing investigation, individuals may not receive notice as to how their information will be used or disclosed. The use and disclosure of this information is governed by applicable federal law, discovery rules and court orders. On occasions when notice cannot be provided or is not required, the FDIC provides constructive notice through its general Privacy Policy and PIAs, including this one.

# 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?**

BODOTS does not collect information directly from individuals who are involved in Board matters and does not provide them direct access to the system.

The FDIC provides individuals the ability to have access to their PII maintained in its systems of records as specified by the Privacy Act of 1974 and FDIC Circular 1360.20. Access procedures for this information system are detailed in the SORN(s) listed in Question 2.2 of this PIA. The FDIC publishes

its System of Records Notices (SORNs) on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and 12 C.F.R. § 310. The FDIC publishes access procedures in its SORNs, which are available on the FDIC public-facing website. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests. Depending on the nature of the records being processed (and any applicable Privacy Act or FOIA exemptions), FDIC may be unable to provide individual access to records as they could inform the subject of an ongoing investigation or reveal a prospective enforcement or investigative interest on the part of FDIC.

In addition, BODOTS maintains information from government agencies or other third-party entities. The system does not have procedures for individual access in these cases. Individuals should contact these source entities directly for access to their personal information.

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

BODOTS does not collect information directly from, or provide direct system access to, individuals who are subjects of FDIC Board matters.

Additionally, the FDIC allows individuals to submit requests 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. These requests are subject to any applicable Privacy Act or FOIA exemptions intended to prevent harm to FDIC's investigation and enforcement interests.

In cases where BODOTS processes third-party data from government agencies or other entities, the FDIC does not have the ability to implement procedures to allow individuals to correct inaccurate or erroneous information within the tool suite. Individuals should contact the government agency or third-party entity directly to correct any erroneous or inaccurate information.

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

BODOTS does not collect information directly from, or provide direct system access to, individuals who are subjects of Board matters.

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(s) listed in Section 2.2 of this PIA. This is in accordance with the Privacy Act and FDIC Circular 1360.20.

In some cases, BODOTS derives data from government agencies or other third-party entities. Individuals should contact these entities directly for access to their personal information.

# Privacy Risk Analysis: Related to Access and Amendment

**Privacy Risk**: Individuals who are subjects of FDIC Board matters may not be able to correct or amend inaccurate information about themselves.

**Mitigation**: Individuals may request access and amendment to their personal information in accordance with the Privacy Act and the FDIC's Privacy Act regulations, at 12 C.F.R. § 310.3 and 310.4. However, some FDIC Board records may be exempt from access under the Privacy Act or FOIA in order to prevent harm to the investigative or enforcement process. Providing individual access to such records may reveal investigative or

enforcement interests on the part of FDIC. Access to records could also permit the individual who is the subject of a record to impede the Board's deliberation or FDIC's investigation and/or tamper with witnesses or evidence. In cases where BODOTS derives data from government agencies or other third-party entities, individuals should contact the source entities and agencies that originated their data to access and amend their information.

# 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 Privacy Impact Assessments (PIAs). The Privacy Program looks across all FDIC systems and programs to identify potential areas of privacy risk. The PTA is used to assess systems or sub-systems, determine privacy compliance requirements, categorize systems, and determine which privacy controls should be assessed for each system.

**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 1360.20, "The Federal Deposit Insurance Corporation (FDIC) Privacy Program"). PIAs are posted on FDIC's public-facing website, 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?**

Contractors provide system maintenance support for BODOTS as requested. Due to 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.**

All FDIC users of BODOTS receive annual Information Security and Privacy Awareness training, which helps ensure PII is handled and safeguarded appropriately. In addition, ESS provides in-house training for all its systems, which addresses (among other things) security requirements and protecting the privacy and confidentiality of information maintained in BODOTS.

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 12 C.F.R. § 310. Disclosures are tracked and managed using the FDIC's FOIA solution.

**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 12 C.F.R. § 310.

**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 12 C.F.R. § 310.

# Privacy Risk Analysis: Related to Accountability

**Privacy Risk**: Inadvertent or malicious actions taken on a particular Board matter may not be traceable back to an individual.

**Mitigation**: The Board of Directors Records Tool Suite implements auditing controls whereby actions taken by a user on a particular matter are tracked. This auditing feature maintains accountability of an action taken by an authorized user. Specific audit trails record the actions of all users to include specific audit information (user ID, time/date, and action).

## 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 and regulations: the Federal Deposit Insurance Act as amended, 12 USC § 1811 et seq. and the regulations adopted by the Board of Directors and codified at 12 CFR Ch. III. The context of the records being processed determines the specific legal authority that permitted their original collection. Additionally, the nature and context of the data dictates whether/which FDIC system of records notice (SORN) applies. For example, any records relating to administrative enforcement or personnel actions taken by the FDIC Board of Directors, standing committees or other delegated

officials would be covered by FDIC-003, Administrative and Personnel Action Records,[38] whereas any Privacy Act records relating to resolution and receivership matters would be covered by the FDIC-013, Insured Financial Institution Liquidation Records.[39] The FDIC Identity, Credential and Access Management Records SORN[40] covers any logs, audits, or other security data regarding use of FDIC information technology resources, including access to and use of the ESS tools and resources by authorized individuals.

# Privacy Risk Analysis: Related to Authority

**Privacy Risk**: There are no identifiable privacy risks related to authority for BODOTS.

**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 personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection?**

BODOTS only collects information for which the FDIC has the authority to collect and that is relevant and necessary to execute the Board of Directors operations detailed in Section 9. BODOTS leverages an access control system to restrict user view and edit rights to the minimum necessary to perform daily work tasks, based on predefined roles and restrictions on FDIC division and regulatory authority. This includes limiting access to the BODOTS and data contained therein to only those authorized users with a need-to-know. Additionally, BODOTS has the capability to generate a robust audit trail of all user activity, as detailed above in Section 4.

Further, through the conduct, evaluation and review of privacy artifacts,[41] 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?**

BODOTS only collects information for which the FDIC has the authority to collect and that is relevant and necessary to execute the Board of Directors operations detailed in Section 9. BODOTS leverages an access control system to restrict user view and edit rights to the minimum necessary to perform daily work tasks, based on predefined roles and restrictions on FDIC division and regulatory authority. This includes limiting access to the BODOTS and data contained therein to only those

[38] FDIC SORN-003, Administrative and Personnel Action Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[39] FDIC SORN-013, Insured Financial Institution Liquidation Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[40] FDIC SORN-035, FDIC Identity, Credential and Access Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[41] Privacy artifacts include Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), and System of Record Notices (SORNs).

authorized users with a need-to-know. Additionally, BODOTS has the capability to generate a robust audit trail of all user activity, as detailed above in Section 4.

All FDIC personnel are required to complete annual information security and privacy awareness training. This is required for BODOTS end users prior to gaining access to the system. This online training addresses how to determine what constitutes PII and how to handle it. In addition, breach prevention is addressed in the training. BODOTS has built-in user security features to help manage and restrict what information users have access to on a "need-to-know" basis and according to their work responsibilities. These user security permissions are controlled by BODOTS system administrators.

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. Whenever possible, users access information in the originating systems. Information is not uploaded into BODOTS except as needed to support authorized business purposes as described above.

**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.**

The retention period for Board records in the system is permanent, as set forth in the associated FDIC Records Retention Schedule, Series 1 – Administration and Management, Organizational Documentation, Board of Directors' Meetings, Official Meeting Minutes/Jackets – found in the FDIC Records and Information Management (RIM) Policy Manual with a Retention Code of EIS1014, Board of Directors Records. The Division of Administration (DOA) Records and Information Management Unit (RIMU) and ESS will coordinate to determine appropriate retention and disposition procedures for documents maintained within the FDIC's communication and collaboration tool.

Procedures for disposition of the data at the end of the retention period are established in accordance with FDIC Records Schedules in conjunction with NARA guidance. For example, hard copies of any paper materials scanned into the system will be retained in accordance with FDIC Records Schedules or returned to the originating Division or Office for retention.

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 personally identifiable information (PII) for testing, training, and research? Does the information system or project implement controls to protect PII used for testing, training, and research?**

The FDIC is in the process of developing an enterprise test data strategy to reinforce the need to mask or utilize synthetic data in the lower environments whenever possible, and ensure all environments are secured appropriately based on the impact level of the information and the information system.

# Privacy Risk Analysis: Related to Minimization

**Privacy Risk**: There is a risk that Board records stored in the BODOTS could be duplicative of information in source systems and could be retained for longer than necessary to accomplish the purpose for which the information was originally collected.

**Mitigation**: FDIC maintains and disposes of the records in the Board of Directors' Operations Tool Suite according to the records schedules and policies discussed in Section 6. Within the tool suite, BODREC serves as the authoritative recordkeeping system for Board matters, and Docket-SP as the authoritative indexing system for administrative action records. ESS uploads only the minimum amount of information necessary to accurately index action records, record Board determinations, and execute other Board operations. Any copies of BODREC data maintained on the FDIC's online collaboration tool must be deleted when no longer needed for reference. The FDIC's communication and collaboration tool also has built-in retention schedules that can be implemented to notify users when documents have reached its expiration and to automatically delete or allow users to manually delete documents when no longer needed. ESS plans to work with the Division of Administration (DOA) Records and Information Management Unit (RIMU) to determine appropriate retention and disposition procedures for documents maintained on the FDIC's communication and collaboration tool and will then configure retention schedules within the tool accordingly.

## 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?**

BODOTS does not collect information directly from individuals who are subjects of Board matters, but instead collects PII from other agency recordkeeping systems or third parties. The FDIC allows individuals to request access and amendment to their personal information in accordance with the Privacy Act and the FDIC's Privacy Act regulations, at 12 C.F.R. § 310.3 and 310.4. In cases where PII is derived from government agencies or other third-party sources, the FDIC does not have the ability to implement procedures to correct inaccurate or erroneous information. Individuals should contact these third parties directly to correct any erroneous or inaccurate information. Additionally, the FDIC does not make decisions regarding individuals based on the PII received from third parties.

**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 validates the configuration of 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**: There is a potential risk associated with data quality and integrity because erroneous or inaccurate information could be entered or uploaded into BODOTS.

**Mitigation**: FDIC mitigates this risk by verifying the accuracy and completeness of information to the extent necessary for accurately recording, indexing and reporting on information about Board matters. This includes carefully recording and confirming key data, such as the dates, Board deliberations/determinations, names of parties involved, and supplemental materials associated with each Board meeting and matter, including those that may pertain to individuals. ESS vets the Board meeting minutes and accompanying materials with the Board and receives their final approval prior to uploading the official, signed copies into BODOTS. ESS does not manually key PII into BODOTS (with the exception of the name field in Docket-SP). Instead, the PII contained in BODOTS is generally located within the contents of files/documents that are uploaded by ESS, after undergoing a multi-layered review and vetting process as applicable.

## 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 personally identifiable information (PII) prior to its collection.**

Since BODOTS does not collect information directly from individuals involved in Board matters, it is not always possible or practical to provide notice and choice opportunities to individuals prior to the collection and processing of their information within the system. Wherever feasible, FDIC provides notice and relevant consent options to individuals at the original point of collection. For example, in cases where BODOTS derives PII from other FDIC record systems, the FDIC provides notice to individuals at the original point of collection through the respective Privacy Act Statements, SORNs, and PIAs, as applicable, for those source systems. This notice explains the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of PII.

When BODOTS derives third-party data from a government agency or other third-party entity, the FDIC does not have the ability to provide privacy notices prior to the agency's processing of individuals' PII. In such cases it is incumbent upon the source entity to provide any applicable, required notices to the individuals from whom they collected the information. Individuals should review the relevant third party's privacy notices. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII.

For information that is collected pursuant to a request from the FDIC, notice is provided as part of the request (e.g., in a letter request, or in the document outlining the compulsory process request). Litigants in civil cases are made aware that courts may compel FDIC to search for and produce agency records pertaining to them and their claims during the litigation process. In addition, this PIA serves as notice to the general public about FDIC's collection and use of information in BODOTS.

When FDIC collects information pursuant to a court order or as part of an ongoing investigation, individuals may not receive notice (or consent opportunities) as to how their information will be used or disclosed. The use and disclosure of this information is governed by applicable federal law, discovery rules, and court orders. When notice cannot be provided or is not required, the FDIC provides constructive notice through its general Privacy Policy and PIAs, including this one.

**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.**

Since BODOTS does not collect information directly from individuals involved in Board matters, it is not always possible or practical to provide notice and choice opportunities to individuals prior to the collection and processing of their information within the system. Wherever feasible, FDIC provides notice and relevant consent options to individuals at the original point of collection. In such cases, the FDIC describes in the Privacy Act Statement and other privacy notices the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of PII. Refer to Section 8.1 above for additional details.

**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.**

The project or system only uses PII for the purposes listed in Section 9.1. This PIA and the SORN(s) listed in 2.2 serve as notice for all uses of the PII. Additionally, the FDIC ensures that individuals are aware of all uses of PII not initially described in the public notice, at the time of collection, in accordance with the Privacy Act of 1974 and the FDIC Privacy Policy.

**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/policies/privacy/index.html, instructs individuals 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 is risk related to individual participation because BODOTS does not collect data directly from individuals. Individuals may not be aware and/or have provided explicit consent for the collection and use of their information within BODOTS.

**Mitigation**: This PIA and the associated SORNs detailed above provide transparency to the public regarding the collection and use of information in BODOTS. In addition, FDIC provides notice to individuals at the original point of data collection wherever possible. In cases where Board records include PII derived from other FDIC Privacy Act systems of records (SORs), the FDIC provides notice to individuals at the original point of collection through the respective SORNs and Privacy Act Statements (PAS) for those source systems. For example, for information that is collected pursuant to a request from the FDIC, notice is provided as part of the request (e.g., in a letter request, or in the document outlining the compulsory process request). In cases where BODOTS derives PII from government agencies or other third parties, those entities are responsible for providing any applicable, required notices to the individuals from whom they initially collected the information. When FDIC collects information pursuant to court order or as part of an ongoing investigation, individuals may not receive notice (or the opportunity to consent) as to how their information will be used or disclosed. The use and disclosure of this information is governed by applicable federal law and court orders. When notice and/or consent opportunities cannot be provided or are not required, the FDIC provides constructive notice through its general Privacy Policy and PIAs, including this one.

# 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.**

As the docket clerk for the Board and the FDIC's Administrative Officer in all administrative enforcement actions, ESS indexes and maintains the official records of all enforcement actions, whether contested or stipulated. ESS also produces certificates of insurance for insured financial institutions on behalf of the Board. Additionally, as the Board's secretary and record custodian, the Executive Secretary Section creates and compiles FDIC Board of Directors meeting minutes and other related documentation in order to accurately record the discussions that take place during Board meetings. Content recorded from Board meeting discussions and supporting documentation may contain agency sensitive information and PII. These documents contain important precedent and historical information that can be used to facilitate the Board's subsequent decision-making process.

**9.2 Describe how the information system or project uses personally identifiable information (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 is mandatory for all staff and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

Within the Legal Division, a limited number of staff in the following groups have authorized access to information maintained in the components of BODOTS as described below:

Legal Division, Executive Secretary Section (ESS): ESS staff have access to BODOTS to produce, edit, and store Board of Director meeting minutes and documents relevant to Board of Directors' Meetings, and to search for relevant information from board meetings at the request of the Board or other executives. Authorized ESS users also have access to BODOTS to produce certificates of insurance for insured financial institutions; electronically share relevant materials with Board members; and to index, upload and archive administrative enforcement actions, legal pleadings and other associated court/case documents.

Legal Division, Information Technology Unit (LITU): LITU staff may be granted access to BODOTS for support purposes and to assist with conducting system administration functions such as adding users to the system, system upgrades, and troubleshooting user reported problems.

Access to BODOTS material is restricted and role-based according to job function and contingent on a business need to know. All users must have the approval by the Program Manager in the FDIC Legal Division in order to gain access to the data.

FDIC also grants ex officio Board members access to the FDIC's online communication and collaboration portal in order to review Board-related materials.

In addition, a limited number of users in the FDIC Division of Information Technology (DIT) may have access to certain components of the tool suite for system administration and troubleshooting purposes. They generally are unable to view/access the database containing PII.

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.

The BODOTS system owners/program managers serve as the primary source of information for data definition and data protection requirements and are responsible for supporting FDIC's corporate-wide view of data sharing. Additionally, all FDIC employees and Board members who have authorized access to information in BODOTS bear responsibility for assuring proper use of the data and abiding by the FDIC data protection rules. All FDIC users with access to the system must complete annual Information Security and Privacy Awareness Training. This training has specific information regarding the compromise of data and the prevention of misuse of data.

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

Users are granted access to specific roles set within the Board of Directors Records tool suite. All users who have access to BODOTS must have the approval of their Manager/Supervisor, as applicable, and the FDIC Program Manager/System Owner for the platform to which they require access. Additionally, the functional security of the systems within the tool suite limits a user's access to specific functions and regulates a user's ability to update or upload data for a specific function based on job responsibilities and limited to information needed to perform position duties.

All access is granted 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.

**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?**

No, the project does not aggregate data to make programmatic level decisions.

**9.6 Does the information system or project share personally identifiable information (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.**

The online communication and collaboration component of BODOTS allows ESS to share Board-related materials with ex officio Board members. This sharing of information is necessary to allow the FDIC Board to execute its statutory responsibilities pursuant to the FDI Act and the governing bylaws of the FDIC.

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 1360.20 '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 is 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 a risk that disclosures of information in BODOTS could be incompatible with the original purposes for which the information was collected.

**Mitigation**: To mitigate this risk, BODOTS restricts access to data to users with a "need-to-know" who require the information to perform their Board-related job responsibilities. Any information disclosures are initiated by authorized FDIC personnel who have a responsibility to share the information for purposes that are compatible with the purpose for which the PII was originally collected and/or that are otherwise legally authorized or required. Additionally, any information disclosures are made based on the nature of the records and, as applicable, pursuant to the routine uses and exemptions in the SORNs that cover the source records.

# 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 personally identifiable information (PII).**

The FDIC Privacy Section maintains an inventory of all programs and information systems identified as collecting, using, maintaining, or sharing PII.

**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 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 related to security for BODOTS.

**Mitigation**: No mitigation actions are recommended.