FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for
Equal Employment Opportunity (EEO) Complaints Solution

April 29, 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[1], which describes FDIC's activities that impact privacy, the authority for collecting PII, and the procedures to access and have PII amended or corrected if necessary.

SYSTEM OVERVIEW

Pursuant to the regulations of the Equal Employment Opportunity Commission (EEOC), 29 CFR Part 1614, the U.S. Equal Employment Opportunity Commission's Management Directive 110, and FDIC Directives 2710.1, Equal Opportunity Policy, the FDIC Office of Equal Employment Opportunity (OEEO) works to ensure equal employment opportunity for all employees and applicants for employment.

Claims within the jurisdiction of the EEOC include those based on race, color, religion, sex, national origin, disability (physical and/or mental), age (40 years or older), genetic information and retaliation for participating in the EEOC discrimination complaint process or opposing discriminatory practices. Any complaints submitted to OEEO that represent a potential conflict of interest, e.g., filed against OEEO staff or the Chairman, are segregated from other complaints and processed by FDIC's Legal Division.

Before a formal complaint can be filed, an employee, former employee, or applicant for employment ("aggrieved individual") must first consult an EEO Counselor in order to try to informally resolve the matter. The formal complaint must be submitted in writing and signed by the Complainant or their representative, within 15 calendar days of receipt of the Notice of Right to File from the EEO Counselor.

Upon receipt of the formal complaint, the OEEO reviews the complaint, designates the date it was received, and identifies the claims that have or have not been accepted for investigation. If the claims are not accepted for investigation, a Final Agency Decision dismissing those matters is issued. Such dismissal is in accordance with the applicable EEOC regulations at 29 C.F.R. part 1614. If a portion of a complaint is dismissed, the Complainant may not appeal the dismissal until the hearing before an Administrative Judge at the EEOC or the final agency action is issued on the complaint. The final agency action, a Final Agency Order or Final Agency Decision, includes a statement of the aggrieved individual's appeal rights and the time limits within which to exercise those rights.

For issues that have been accepted for investigation, the aggrieved individual is advised of the name of the investigative firm and investigator assigned to conduct the investigation. Upon completion of the investigation, the aggrieved individual is issued a Report of Investigation along with a letter, which may offer the aggrieved individual the opportunity to participate in the EEO mediation program. If the aggrieved individual is offered mediation, they must indicate their acceptance or declination of the mediation within 15 days from receipt of the letter. The letter also advises the aggrieved individual of their right to request a hearing before an EEOC Administrative Judge or a Final Agency Decision without a hearing based on the evidence contained in the Report of Investigation. The final agency action is issued by the Chairman or agency official designated by the Chairman; in most cases, this authority has been delegated to the Director, OEEO. The aggrieved individual must indicate their election of a hearing or a Final Agency Decision within 30 days from receipt of the letter.

If the aggrieved individual is offered and elects mediation, OEEO will contact them, or their representative, to arrange the mediation session. Mediation is voluntary and is conducted by an independent, experienced mediator.

[1] www.fdic.gov/privacy

If mediation is not successful, then the processing of the aggrieved individual's complaint shall resume. If the aggrieved individual requests a hearing before the EEOC, they must send a written request directly to the appropriate EEOC office and notify the FDIC that they have requested a hearing. The EEOC assigns an Administrative Judge to the case. The EEOC Administrative Judge advises the aggrieved individual, or their representative, of the hearing process and procedures.

The EEOC Administrative Judge may issue a decision with or without a hearing. After receiving the decision of the EEOC Administrative Judge, the FDIC issues a Final Agency Order implementing, modifying or rejecting the EEOC Administrative Judge's decision. If the aggrieved individual requests a Final Agency Decision without a hearing, the FDIC will issue a Final Agency Decision based on the evidence in the Report of Investigation.

If the aggrieved individual does not agree with the final agency action, Final Agency Order or Decision, they may appeal the action to the EEOC, Office of Federal Operations, or file a civil action. The Final Agency Order or Decision provides the appeal rights and the notice of the right to file a civil action in a U.S. District Court and the applicable time limits for filing an appeal and lawsuit.

Special Procedures:

- Collective Bargaining Agreement—The FDIC has a Collective Bargaining Agreement with the National Treasury Employees Union ("NTEU") that permits allegations of discrimination to be raised under the negotiated grievance procedure. Therefore, Bargaining Unit employees covered by the negotiated grievance procedure who believe they have been discriminated against may pursue the matter under either the FDIC's administrative discrimination complaint process or the negotiated grievance procedure, but not both. An election to proceed under the FDIC's administrative discrimination complaint process is indicated only by the filing of a written formal complaint; use of the Informal Counseling Procedures does not constitute an election. Employees who elect to file a grievance that alleges employment discrimination through the negotiated grievance procedure may not thereafter file a formal complaint through the FDIC's administrative discrimination complaint process on the same matter.
- Class Complaints—A class is defined as a group of employees, former employees, or applicants who allege that they have been or are being adversely affected by an FDIC policy or practice that discriminates against the group on the basis of their race, color, religion, sex, national origin, age, genetic information, or disability. A class complaint is filed on behalf of the class by the agent(s) of the class. Individuals wishing to initiate a class complaint must contact OEEO for assignment to an EEO counselor.
- Age Complaints—Individuals who wish to file a complaint of discrimination on the basis of age may either seek counseling and file a formal administrative complaint, as described above, or file suit in the appropriate U.S. District Court after giving the EEOC not less than 30 days' notice of his or her intent to file such an action.
- Equal Pay Act Complaints—Individuals have the right to file a civil action under the Equal Pay Act (sex-based wage discrimination) directly in U.S. District Court, without filing any Notice of Intent to Sue and without participating in the administrative complaint process. In connection with the Equal Pay Act, liquidated damages are available if a willful violation of the law is proven.
- Mixed Case Complaints—A mixed case complaint is a complaint of employment discrimination based on race, color, religion, sex, national origin, age, genetic information, or disability, related to or stemming from a personnel action that can be appealed to the Merit Systems Protection Board (MSPB). Some examples of these actions include, but are not limited to, termination, reduction in grade, and suspension of more than 14 days. An individual may file either a mixed case appeal with MSPB or a mixed case complaint through the FDIC's administrative discrimination complaint process. However, an individual may not file both. An election to proceed under the FDIC's administrative discrimination complaint process or MSPB, is indicated by the filing of a mixed case complaint or a mixed case appeal, respectively. Special procedures and appeal rights govern the processing of mixed cases.
- Sexual Orientation and Parental Status,—The EEOC has jurisdiction over sex based claims including sexual orientation. These claims, as well as claims based on status as a parent, can also be filed under the FDIC Circular 2710.4, FDIC Discrimination Complaint Process. If an individual wishes to pursue an allegation of discrimination under this policy, they should contact an EEO Counselor within 45 days of the alleged discrimination.

Remedies may include:

- posting a notice to all employees advising them of their rights under the laws EEOC enforces and their right to be free from retaliation;
- corrective or preventive actions taken to cure or correct the source of the identified discrimination;
- nondiscriminatory placement in the position the victim would have occupied if the discrimination had not occurred;
- compensatory damages;
- back pay (with interest if applicable) and lost benefits; and
- stopping the specific discriminatory practices involved.

The FDIC uses the EEO complaints solution to:

1. Manage the caseload of alleged employment discrimination, retaliation, and alternative dispute resolution matters;
2. Store records associated with EEO complaints; and
3. Generate two statutorily-required reports:
    - No Fear Act reports—The Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act) or Public Law 107-174 seeks to discourage federal managers and supervisors from engaging in unlawful discrimination and retaliation. Federal agencies are required to post quarterly on their public Web sites certain summary statistical data relating to equal employment complaints filed against the respective agencies. Additionally, federal agencies are required to submit an annual report to the Speaker of the House of Representatives, the President Pro Tempore of the Senate, the Committee on Governmental Affairs of the Senate, the Committee on Government Reform of the House of Representatives, each committee of Congress with jurisdiction relating to the agency, the Equal Employment Opportunity Commission, and the Attorney General.
    - EEO 462 Reports—The U.S. Equal Employment Opportunity Commission produces an Annual Report on the Federal Workforce that includes, among other data, information on federal equal employment opportunity complaints and Alternative Dispute Resolution activities (EEOC Form 462). This data is collected from the FDIC and other agencies in the Annual Federal Equal Employment Opportunity Statistical Report of Discrimination Complaints (EEOC Form 462).

The EEO complaints solution is maintained by a third-party contractor that is contractually obligated to comply with FDIC security and privacy requirements.

PRIVACY RISK SUMMARY

In conducting this PIA, we identified potential privacy risks, which are outlined below. As indicated, recommendations to mitigate those risks were addressed with stakeholders during the assessment. The privacy risks are categorized within the following privacy functional areas:

Minimization

Privacy Risk: There is a risk that more information may be collected than necessary to resolve an EEO complaint.

Mitigation: The risk of over collection is mitigated by OEEO procedures to collect and maintain information in the EEO complaints solution that is relevant to the investigation of a particular complaint, and destroying the records ten years after a complaint case is closed.

Transparency

Privacy Risk: There is a risk that individuals associated with a filed complaint may not be aware the full extent of the information collected and maintained within the EEO complaints solution.

Mitigation: Individuals who submit a complaint receive a Privacy Act Statement that describes the authority, purposes, disclosure, retention, and access and correction provisions that may apply to information

associated with a complaint. For all others, the FDIC provides public notice regarding the EEO complaints process and IT solution in the EEOC/GOVT-1 Equal Opportunity in the Federal Government Complaint and Appeal Records SORN and this PIA.

Use Limitation

Privacy Risk: There is a risk that the information may be used for purposes not consistent with the original purpose or to retaliate against an aggrieved individual.

Mitigation: The risk of inappropriate use of information in the EEO complaints solution is mitigated through the use of role-based access controls and EEO training. The risk of FDIC inappropriately misusing the information against an aggrieved individual by way of retaliation is mitigated by the legal prohibition against retaliation, and the opportunity for any aggrieved individual who believes they have been subject to retaliation to file a complaint with the Office of Special Counsel (OSC). OSC has the authority to investigate allegations of retaliation and may seek corrective or disciplinary action when warranted.

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?

The system contains information related to claims of discrimination. The information collected varies based on the nature of the complaint, the sources of information used to investigate the complaint, and the results of the investigation.

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	☒	☐

PII Element	Yes	No
Biometric Identifiers (e.g., fingerprint, voiceprint)	☐	☒
Photographic Identifiers (e.g., image, x-ray, video)	☐	☒
Other (Specify: sex, national origin, race, age, religion, disability, genetic information, marital status, parental status, pregnancy, retaliation, and color)	☒	☐

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

Data Source	Description of Information Provided by Source
Individuals and Form 2710, Formal Complaint of Discrimination	Complaint records contain personal contact information about the complainants and potentially private information necessary to address the allegations raised against the FDIC.
Co-workers, supervisors, witnesses, legal representatives and others with knowledge regarding the allegations of discrimination	Third parties with knowledge of the allegation of discrimination may provide information relevant to the EEO complaint filed by an aggrieved individual.
HR systems	Records from HR systems such as those that capture applicant flow, performance evaluations, pay, training and other general employment records may be collected and reviewed as part of the investigation into allegations raised against the FDIC.

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

The ATO was issued on January 30, 2018 and will be 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 project: EEOC/GOVT-1 Equal Opportunity in the Federal Government Complaint and Appeal Records, which covers records compiled during the investigation of age and equal pay discrimination cases and during the investigation and hearing of complaints filed under section 321 of the Government Employees Rights Act of 1991. These records include:

a. Documents submitted by charging party or complainant such as charge of discrimination, personal interview statement, and correspondence.

b. Documents submitted by employer such as statement of position, correspondence, statements of witnesses, documentary evidence such as personnel files, records of earnings, employee benefit plans, seniority list, job titles and descriptions, applicant data, organizational charts, collective bargaining agreements, petition to revoke or modify subpoena.

c. Records gathered and generated by EEOC in the course of its investigation and in complaints filed under section 321 of the Government Employees Rights Act of 1991, during the hearing, such as letters of referral to state fair employment practices agencies, correspondence with state fair employment practices agencies, witness statements, investigator's notes, investigative plan, report of initial and exit interview, investigator's analyses of evidence and charge, subpoenas, decisions and letters of determination, conciliation agreements, correspondence and any additional evidence gathered during the course of the investigation.

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

The SORN(s) referenced in 2.2 do not require amendment or revision. 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.

Individuals that file a formal complaint receive a Privacy Act Statement when they receive Form 2710/01, Formal Complaint of Discrimination. Additional information on how PII is handled is provided in supplementary guidance.

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 1213.01, FDIC Forms Management Program.

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: There is a risk that individuals associated with a filed complaint may not be aware the full extent of the information collected and maintained within the EEO complaints solution.

Mitigation: Individuals who submit a complaint receive a Privacy Act Statement that describes the authority, purposes, disclosure, retention, and access and correction provisions that may apply to information associated with a complaint. For all others, the FDIC provides public notice regarding the EEO complaints process and IT solution in the EEOC/GOVT-1 Equal Opportunity in the Federal Government Complaint and Appeal Records SORN and this PIA.

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?

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 or projected 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 FDIC Circular 1360.20. 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.

Aggrieved individuals may also contact OEEO staff via email, telephone, or mail to request information on the status of their case.

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

The FDIC allows individuals 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. The FDIC publishes its 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 FDIC Circular 1360.20. 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.

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

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.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: There are no identifiable risks associated with accountability for the EEO complaints solution.

Mitigation: No mitigation actions are recommended.

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). A PTA is used to determine whether a PIA is required under the E-Government Act of 2002 and the Consolidated Appropriations Act of 2005. A PIA is required for: (1) a new information technology (IT) system developed or procured by FDIC that collects or processes personally identifiable information (PII); (2) a substantially changed or modified system that may create a new privacy risk; (3) a new or updated rulemaking that may affect the privacy of PII in some manner; or (4) any other internal or external electronic collection activity or process that involves PII.

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). 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 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, appropriate confidentiality agreements have been completed and signed for contractors who work on the 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.

The FDIC Privacy Program also 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.

In addition to the annual privacy training, OEEO personnel are required to take system-specific training for new system users and refresher training and training for new features as they are released for existing users.

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 (SAOP) Report 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?

A system administrator grants access to authorized users based on a request from the authorized user's manager. An audit log captures who is granted access, by whom, and when. User access is further controlled and restricted according to specific user and administrative roles that have been defined and established within the EEO solution. Each case within the EEO complaint solution has an audit trail to track modifications and who made the changes (by person and date/time stamp).

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 when 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?

Disclosures are not made directly from the EEO solution. The FDIC maintains an accurate accounting of disclosures of information held in each system of record under its control, in accordance with the Privacy Act of 1974 and FDIC Circular 1360.20. Disclosures are tracked and managed using FDIC's Freedom of Information Act 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 FDIC Circular 1360.20.

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 FDIC Circular 1360.20.

Privacy Risk Analysis: Related to Accountability

Privacy Risk: There are no identifiable risks associated with accountability for the EEO complaints solution.

Mitigation: No mitigation actions are recommended.

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 personally identifiable information (PII) are legally authorized through the conduct and documentation of Privacy Impact Assessments (PIA) and the development and review of System of Records 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:

- 42 U.S.C. 2000e-16: prohibits discrimination in federal government employment
- No FEAR Act, Public Law 107-174: creates accountability for antidiscrimination violations and EEO complaint reporting
- 29 CFR 1614: provides for equal employment opportunity programs

Employees and applicants for employment who believe that they have suffered discrimination or retaliation may file a complaint under one or more of the following statutes:

- Title VII of the Civil Rights Act of 1964, as amended, 42 U.S.C. § 2000e-16, prohibits employment discrimination on the bases of race, color, religion, sex, national origin, and in reprisal for participating in a statutorily protected activity;
- The Age Discrimination in Employment Act ("ADEA") of 1967, as amended, 29 U.S.C. § 633a, prohibits employment discrimination on the basis of age (40 years or older);
- The Rehabilitation Act of 1973, as amended, 29 U.S.C. §§ 791-794e, prohibits employment discrimination on the bases of mental or physical disabilities;
- The Equal Pay Act of 1963, as amended, 29 U.S.C. § 206(d), prohibits sex-based wage discrimination; and
- Title II of the Genetic Information Nondiscrimination Act (GINA)

Privacy Risk Analysis: Related to Authority

Privacy Risk: There are no identifiable risks associated with authority for the EEO complaints solution.

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?

FDIC has EEO processing procedures that establishes what information should be collected based on the allegation in the complaint.

Additionally, through the conduct, evaluation and review of privacy artifacts,[2] 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?

Additionally, through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that the collection and retention of PII is limited to the PII that has been legally authorized to collect.

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 an 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.

EEO complaint records are retained for 10 years after closure of case, in accordance with FDIC Circular 1210.01 FDIC Records and Information Management Program, which is informed by the Federal Records Act and NARA regulations.

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 more information may be collected than necessary to resolve an EEO complaint.

[2] Privacy artifacts include Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), and System of Record Notices (SORNs).

Mitigation: The risk of over collection is mitigated by OEEO procedures to collect and maintain information in the EEO complaints solution that is relevant to the investigation of a particular complaint, and destroying the records ten years after a complaint case is closed.

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.

Individuals who initiate complaints are required to complete and sign forms that provide the initial information necessary for the processing of a discrimination complaint. Information is entered manually into the system as provided directly by the individual making the complaint. Only designated Super Users can add or modify data. To ensure data accuracy, there are three levels of review: peer review, Complaints Processing Branch management review, and Quality Control Review Committee (QCR) review. Individuals are responsible for keeping the records up to date with their current mailing address, and phone numbers and/the name, address, and daytime phone number of any representative.

Additionally, 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?

The information system or project collects PII directly from the individual. The information system or project collects PII from aggrieved individuals or third parties with knowledge relevant to the complaint. OEEO staff then enter the information into the EEO complaints solution. The FDIC reviews privacy artifacts to ensure each collection of PII is directly from the individual to the greatest extent practicable.

7.3 Describe any administrative and technical controls that have been established to detect and correct PII that is inaccurate or outdated.

To help detect and correct PII that is inaccurate or outdated, there are three levels of review: peer review, Complaints Processing Branch management review, and Quality Control Review Committee (QCR) review. Individuals are responsible for keeping the records up to date with their current mailing address, and phone numbers and/the name, address, and daytime phone number of any representative.

Additionally, 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.

To ensure the integrity of PII,OEEO uses three levels of review: peer review, Complaints Processing Branch management review, and Quality Control Review Committee (QCR) review.

Through its PTA adjudication process, the FDIC Privacy Program uses 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 Security Officer prescribes 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 are no identifiable risks associated with data quality and integrity for the EEO complaints solution.

Mitigation: No mitigation actions are recommended.

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.

Aggrieved individuals authorize the collection, use, maintenance, and sharing of EEO complaint information by seeking redress for an alleged instance of discrimination under EEO authorities. They can choose whether to bring an informal or formal complaint, whether to use the mediation process, and whether to appeal an agency decision of a complaint. Aggrieved individuals must submit a signed, written complaint or submit Form 2710/01, FDIC Formal Complaint of Discrimination to OEEO that contains the initial information necessary for the processing of a discrimination complaints aggrieved individuals have the right to representation and to remain anonymous during the EEO counseling process. Agency witnesses must participate in the EEO investigation process. Upon receipt of information associated with a complaint, OEEO staff enter the information or record into the EEO complaints solution.

When information is collected directly from the individual, the FDIC Privacy Program ensures that Privacy Act (e)(3) statements and other privacy notices are provided, as necessary, to individuals prior to the collection of PII. This implied consent from individuals authorizes the collection of the information provided. Additionally, this PIA and the SORN(s) listed in 2.2 serve as notice of the information collection. Lastly, the FDIC Privacy Program also reviews PIAs to ensure that PII collection is conducted with the consent of the individual to the greatest extent practicable.

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.

Individuals are advised of the potential consequences based on their relationship to the complaint. For example, if authorization to use PII is not provided by an aggrieved individual and a complaint remains anonymous, then OEEO informs them orally or in writing that it is highly unlikely that the complaint can be resolved. If authorization is not provided by a federal employee associated with a complaint, then they are informed orally or in writing that there may be consequences for refusing to participate based on federal regulation.

When the FDIC collects information directly from individuals, it 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.

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 serves 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 FDIC privacy Policies.

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, www.fdic.gov/privacy, 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 are no identifiable risks associated with individual participation for the EEO complaints solution.

Mitigation: No mitigation actions are recommended.

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.

FDIC collects, uses, maintains, and shares EEO complaint information to provide redress for those who believe that they have suffered discrimination on a protected basis.

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.

OEEO publishes specific guidance on how to protect PII and Sensitive Information (SI) during the informal and formal complaint process, including EEO investigations, on the FDIC intranet. The guidance emphasizes that:

- Filing or litigating an EEO complaint does not authorize an aggrieved individual to take home copies of PII, send PII to a personal computer or email account, send PII to an attorney or representative, or submit PII to the EEOC.
- Any aggrieved individual who believes that documents with PII need to be provided to an EEO investigator, an individual's representative, or to the EEOC in support of an EEO complaint should coordinate with an OEEO EEO Counselor or EEO Specialist on how to appropriately provide/preserve these documents as evidence without putting PII at risk unnecessarily.
- PII should be properly redacted such that the aggrieved individual can provide needed evidence without violating FDIC policies, and review documents to make certain that all appropriate redactions have been made.

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.

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

A system administrator grants access to authorized users based on a request from the authorized user's manager. User access is further controlled and restricted according to specific user and administrative roles that have been defined and established. For example, the EEO complaint caseload of the Legal Division and OEEO are segregated so that users are only able to access EEO complaints within their respective caseloads.

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?

The EEO complaint solution does not aggregate or consolidate data in order to make determinations or derive new data about individuals. The EEO complaints solution may searched to show trends or aggregate new data. For example, certain aspects of the system do trace transaction histories that indicate that OEEO staff has performed some work or action, and this may be used in a case review. Similarly, reports may be run to help identify whether there are any Corporation-wide patterns that management should address. The reports do not contain individual-level PII and there is limited risk of re-identification when aggregated results are disclosed outside the EEO complaint solution.

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 information collected and maintained by the EEO complaints solution may be shared externally pursuant to the routine uses described in the SORN EEOC/GOVT-1 Equal Opportunity in the Federal Government Complaint and Appeal Records, referenced in 2.2.

Further, 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, Privacy Program, 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.

Guidance is provided on how to protect PII and Sensitive Information. Complainants are provided notice of their responsibility of securing PII and SI on the FDIC intranet.

Annual Information Security and Privacy Awareness Training is mandatory for all FDIC 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.

Additionally, annual Information Security and Privacy Awareness Training is mandatory for all FDIC staff and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

Privacy Risk Analysis: Related to Use Limitation

Privacy Risk: There is a risk that the information may be used for purposes not consistent with the original purpose or to retaliate against an aggrieved individual.

Mitigation: The risk of inappropriate use of information in the EEO complaints solution is mitigated through the use of role-based access controls and EEO training. The risk of FDIC inappropriately misusing the information against an aggrieved individual by way of retaliation is mitigated by the legal prohibition against retaliation, and the opportunity for any aggrieved individual who believes they have been subject to retaliation to file a complaint with the Office of Special Counsel (OSC). OSC has the authority to investigate allegations of retaliation and may seek corrective or disciplinary action when warranted.

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).

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.

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 Chief Information Security Officer (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 associated with security.

Mitigation: No mitigation actions are recommended.