



**Privacy Impact Assessment (PIA)
for
Enterprise Public Inquiry and Complaints
(EPIC)**



PIA-FDIC-1305

11/25/2019

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 public-facing website¹, 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

The Enterprise Public Inquiry and Complaints (EPIC) effort is an enterprise Software as a Service (SaaS) solution that is built on a cloud-based platform. It is a configured solution to manage constituent complaints and inquiries received by the Federal Deposit Insurance Corporation (FDIC). EPIC is a nationwide system that is accessible online.

EPIC is an automated, cloud-based system that enables FDIC staff to add, update, review, and report on individual cases of constituent complaints, inquiries, suggestions and requests about FDIC data and publications. FDIC receives, responds to, tracks, and reports on complaints and inquiries received from constituents, including financial institutions themselves. The methods of communication to be managed within EPIC include complaints and inquiries received via telephone, email, online forms, mail and fax.

Community Tools

EPIC uses its cloud-based provider's Community Tools. Community Tools enable FDIC divisions, through EPIC, to connect with its stakeholders at a single location. The Community Tools consist of the Citizens' Portal and the Bankers' Portal.

The Citizens' Portal

The Citizen's Portal is a webpage that allows constituents to submit complaints about their financial institutions and check on the status of their complaints. Submitted complaints pass through the EPIC system as cases. The Customer Response Center (CRC) manages cases to conclusion with the financial institutions and reports the financial institutions response back to the constituent.

When constituents register for the portal for the first-time, they are prompted to provide their first name, last name, and their email address. Constituents enter those details and receive an email to confirm their registration. Once constituents have confirmed their registration, they are prompted to enter a random token which is provided to them via email. The token is not stored within cloud service provider (CSP) and the token expires after ten (10) minutes. After entering the token, constituents complete their registration by creating a password. Any subsequent login attempts will generate a token which is sent to the constituent's email address on record. Should constituents become locked of their accounts, constituents must call the CRC, provide the name, case number, and email address given at registration, and a temporary password are sent to the email address on record.² Constituents will still have to dual authenticate before they are able to access their accounts again.

Once constituents have registered to access the Citizens' Portal, they have the ability to submit complaints/inquiries, attach supporting documents, and track the status of complaints or inquiries. The complaints or inquiries may contain PII and financial information. After the complaint or inquiry has been

¹ www.fdic.gov/privacy

² Alternatively, in order to get a temporary password sent to the email address given at registration, users must give the bank name or topic complained about. Additionally, constituents must provide two of the following: name, email, telephone number, or address.

submitted, the FDIC sends the constituent an email or letter confirming the receipt of the complaint or inquiry. The EPIC system directly relays the complaint or inquiry to the relevant bank. Through the Bankers' Portal, the financial institution reviews the complaint or inquiry and is responsible for responding directly to the FDIC for resolution. The financial institution may also respond to the constituent directly.

The Bankers' Portal

The Bankers' Portal allows financial institutions to respond to complaints or inquiries and manage their caseload with the FDIC. Complaints are stored and managed in the EPIC system as cases. Financial institutions respond to those complaints via the Bankers' Portal. To gain access to the Bankers' Portal, bankers must be authenticated by FDICconnect³ (FCX). The financial institutions are then routed from FCX to the Bankers' Portal.

Financial institutions can only access their own complaints or inquiries through the Bankers' Portal. All U.S. financial institutions have certification numbers issued by the FDIC. The FDIC certification number is unique to each financial institution. Designated personnel of financial institutions are provisioned based on their financial institution's certification number. EPIC, through the Bankers' Portal, only allows financial institutions to respond to their own complaints or inquiries.

Once designated personnel of financial institutions have access to the Bankers' Portal, they have the ability view their financial institution's complaints or inquiries and submit responses. The complaints or inquiries may contain PII and financial information.

Complaint /Inquiry Submission and Resolution

EPIC stores information related to the communications and reports to a variety of constituencies on the complaints and inquiries FDIC receives and processes. The categories of individuals who may contact FDIC divisions are: Consumers, Academia, Bankers, Analysts, Congress/Senate/White House, Media/Press, Attorneys, Professionals, FDIC management, FDIC employees, and other Federal, State and Local Agencies.

EPIC uses and maintains PII for FDIC's management of complaints or inquiries. As part of the complaint/inquiry process, PII is collected via incoming calls to the FDIC, the Citizen's Portal, mail, fax, and online forms. For information regarding the submission of complaints/inquiries through the Citizens' Portal, please refer to the section above describing the Citizens' Portal.

Complaints/Inquiries Submitted by Online Forms

Online forms are used by constituents to submit their complaints or inquiries regarding various banking issues and deposit insurance. Once a constituent completes the form and submits their request, the form passes the data to EPIC. A record is created in EPIC and the form submission is attached to the record. The forms collect: requestor type (e.g., academic, banker, consumer), name, email address, phone/fax numbers, title, organization name, state, and description of complaint/inquiry. The form also collects the financial institution's name, city, state, and email address if known. Constituents also have the opportunity to submit and attach supporting documentation.

Once the complaint has been submitted, the FDIC sends the constituent an email or letter confirming the receipt of the complaint/inquiry. Through the Bankers' Portal, the EPIC system directly relays the complaint/inquiry to the relevant financial institution. The financial institution reviews the complaint/inquiry and is responsible for responding directly to the FDIC for resolution. The financial institution may also respond to the constituent directly.

Complaints/Inquiries Submitted by Mail or Fax

Constituents may also mail or fax complaints/inquiries to the FDIC. An FDIC complaint specialist scans the complaint/inquiry, reviews the complaint/inquiry for duplication, and, if appropriate, redacts any

³ See FDICconnect PIA available at www.fdic.gov/privacy.

unnecessary PII. The complaint/inquiry and any supporting documentation are uploaded into EPIC by complaint specialists using the CSP's encrypted email-to-case functionality. The FDIC sends the constituent an email or letter confirming the receipt of the complaint/inquiry. The FDIC directly relays the complaint/inquiry to the relevant financial institution. Through the Bankers' Portal, the financial institution reviews the complaint/inquiry and is responsible for responding directly to the FDIC for resolution. The financial institution may also respond to the constituent directly.

Complaints/Inquiries Submitted by Telephone

Most of FDIC's inquiries are submitted via telephone. Generally, FDIC responds to public inquiries related to its industry analysis publications and data that is published on the FDIC website. FDIC also responds to inquiries related to structuring bank accounts to maximize FDIC deposit insurance. FDIC utilizes EPIC to track the inquiries the agency receives. In doing so, EPIC collects basic contact PII from members of the public.

Complaints cannot be submitted via telephone. Constituents who call the CRC or the FDIC Call Center to submit complaints are directed to the FDIC Complaints website to submit their complaints online.

Complaint Sharing with Federal and State Regulators

FDIC utilizes EPIC to process complaints/inquiries referred from federal and state regulators. For example, if a constituent writes to the Office of the Comptroller of the Currency (OCC) about a financial institution supervised by FDIC, the OCC forwards the incoming constituent correspondence to the FDIC for handling and resolution. Federal and state regulators send complaints to an FDIC shared inbox with all supporting documentation. A complaint specialist monitors this inbox, reviews the complaints, and determines whether the complaints are in the purview of FDIC. All appropriate referrals are manually processed into EPIC by complaint specialists until encrypted email-to-case functionality can be implemented. Complaints/inquiries are resolved based on the standard processes noted above.

EPIC also shares complaints with state and federal regulators. EPIC is integrated with FDIC Extranet to allow one-way communication from EPIC to state banking regulators. Once an MOU is executed, FDIC shares complaints to state financial regulators about financial institutions in their respective states. State financial regulators are allowed to access the Bankers' Portal and see a summary view of the closed complaints for their states' financial institutions without the full complaint details.

For federal financial regulators, complaint specialists send complaints or inquiries contained in EPIC via secure email. These emails are sent to the relevant agency's email mailbox created specifically for the purpose of receiving complaints referred by other financial agencies.

FDIC Internal Users

EPIC stores FDIC employee names to assign user profiles. Some users have administrative access and others standard user access in EPIC. User profiles allow FDIC to track which EPIC users are managing which complaints. EPIC does not have any fixed database fields to record PII. However, FDIC internal users are tasked with scanning incoming paper correspondence, attaching emails, and uploading supporting documentation into EPIC. EPIC requests constituents to provide basic contact information (name, address, email, etc.) so FDIC is able to contact with the resolution of their complaint. However, because EPIC has open fields and upload functionality, constituents have the capability to submit any PII they deem necessary to garner a favorable resolution of their complaints. Any PII identified by FDIC staff that is not necessary to respond to the complaint or inquiry are redacted prior to input into EPIC and/or deleted from EPIC upon discovery. Lastly, constituents can indicate in the incoming correspondence that they do not want their complaints shared with anyone outside the FDIC (i.e., with the financial institution in question).

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:

- Transparency;
- Access and Amendment;
- Accountability;
- Authority;
- Minimization;
- Data Quality and Integrity;
- Use Limitation; and
- Security.

Transparency Risks:

Privacy Risk: Constituents, who erroneously submit complaints to FDIC, may not be aware that FDIC forwards their complaints to the appropriate financial regulator.

Mitigation: FDIC provides Privacy Act Statements to all constituents who submit complaints directly. The Privacy Act Statements inform constituents that FDIC may furnish their complaint “to the Federal or State supervisory authority that has direct supervision over the financial institution.”

Privacy Risk: Constituents, who submit their inquiries telephonically, may be not given Privacy Act Statements and therefore unaware of FDIC’s uses of their PII.

Mitigation: This is no longer a risk. FDIC has implemented oral recitations of EPIC’s Privacy Act Statement prior to the collection of any PII needed for inquiries. Additionally, this PIA and the SORN listed in Section 2.2 serves as notice of the FDIC’s uses of PII received from constituents.

Privacy Risk: Constituents, whose complaints are referred from other financial regulators may be unaware of FDIC’s uses of their PII.

Mitigation: Other financial regulators provide constituents notice that their complaint is shared with other financial regulators for enforcement and statutory purposes. Once FDIC receives the complaint, FDIC sends the constituent an acknowledgement email/letter informing the individual of the complaint referral.

Access and Amendment Risks:

Privacy Risk: The personnel of financial institutions responding to complaints referred by FDIC cannot correct or amend inaccurate information about them contained in EPIC.

Mitigation: The PII of financial institution personnel contained in EPIC is limited to basic contact information such as name, telephone number, and email address. The FDIC does not use these individuals’ PII to deprive them of a right or benefit. Financial institution personnel voluntarily include their PII in responses to FDIC for contact purposes.

Privacy Risk: Constituents may not be able to have their complaint resolved after they have corrected inaccurate information in EPIC because FDIC has already sent the complaint to the relevant financial institution and that financial institution cannot retrieve information on the individual as a result of the inaccurate information.

Mitigation: Once FDIC submits a complaint to a bank, it does not provide the bank with updated information related to that complaint. However, financial institutions notify FDIC when they cannot retrieve information on constituents based on the information provided. An FDIC complaint specialist then writes a personalized letter to the constituent noting that there may have been updated information that was not sent to the financial institution. The FDIC complaint specialist also requests the constituent review and update any inaccurate information submitted in the initial complaint. Once constituents provide FDIC with updated information, FDIC creates an additional complaint in EPIC, links it to the initial complaint, and sends both complaints to the relevant bank for resolution.

Accountability Risk:

Privacy Risk: Constituents are not able to appeal unfavorable resolutions of complaints.

Mitigation: FDIC's statutory mandate is to promote and enforce compliance by FDIC supervised financial institutions with federal consumer protection laws, including those relating to fair lending and unfair and deceptive practices. FDIC carries out this mission by (1) investigating constituent complaints involving financial institutions it supervises; and (2) responding to inquiries from the public and financial institutions about consumer protection and fair lending matters. FDIC's scope of authority does not ordinarily extend to the resolution of complaints involving factual disputes or contractual matters, or matters that have been or are in the process of being litigated.

Authority Risk:

Privacy Risk: FDIC may investigate complaints where it has no legal authority to do so.

Mitigation: FDIC staff reviews complaints to determine if they are in the scope of the FDIC's legal authority. Should FDIC determine that the complaint is not in the scope of its authority, FDIC staff will forward the complaint to the appropriate regulatory authority.

Minimization Risks:

Privacy Risk: More information may be collected than is necessary to resolve an inquiry or complaint.

Mitigation: FDIC limits the scope of information collected in EPIC to the amount of data necessary to act upon the complaints filed. Although the system stores PII provided in the complaint, this information is captured only where it is relevant to the resolution. Any PII identified by FDIC staff as not necessary to respond to the complaint is redacted prior to input into EPIC and/or deleted from EPIC upon discovery.

Privacy Risk: FDIC may retain information longer than necessary.

Mitigation: FDIC retains information contained in EPIC in accordance with its established retention schedule. FDIC divisions are responsible for deleting or archiving information in accordance with the retention schedules. This risk is mitigated because FDIC follows all pertinent records schedules discussed in sections 6.2 and 6.4. In addition, the FDIC Records and Information Management Section provides trainings to inform FDIC programs of proper record retention, disposition requirements, records inventory training, file plan training, and file structure training to ensure that FDIC personnel are aware of all records requirements.

Privacy Risk: The EPIC system may retain un-submitted or incomplete complaints in perpetuity.

Mitigation: For un-submitted complaints, EPIC does not retain data. No data is captured in EPIC until complaints have been submitted. Incomplete complaints, complaints that lack sufficient information for resolution, are retained in accordance with the EPIC retention schedule. FDIC notifies constituents in writing and informs them there is not enough information to investigate the complaint. FDIC then closes out the complaint. Should constituents provide additional information in support of their complaint, the FDIC will create a new complaint in EPIC, link the previous complaint, and forward to the relevant financial institution for resolution.

Privacy Risk: Due to the storage of data on a commercial cloud platform, there could be a failure to adhere to FDIC retention guidelines and schedules.

Mitigation: During the period that the contract with the EPIC CSP is active, the FDIC has direct access to the data and ensures that appropriate retention schedules are followed. After the contract period ends, the CSP is required to adhere to the retention restrictions specified in the contract. Due to the encryption key management service within EPIC's cloud architecture, CSP personnel are incapable of using or redistributing any FDIC data processed and stored within EPIC. Should the CSP be required to access FDIC data to comply with federal law, or with a valid and binding order of a governmental or regulatory body, FDIC will provide the CSP with the necessary encryption keys to access the data. In the rare instances that CSP personnel has access to FDIC data because of a law enforcement requirement or court order, the CSP is obligated, by contract, to abide by all FDIC record retention schedules and privacy/security requirements.

FDIC has access to CSP's cloud hosting environment and may periodically audit the vendor to ensure information is retained per the applicable retention schedules. No additional mitigation actions are recommended.

Data Quality and Integrity Risks:

Privacy Risk: When inquiries are made telephonically, FDIC employees rather than the individuals themselves perform data entry of inquiring individuals' information and this may result in inaccurate information.

Mitigation: Complaint specialists verify the accuracy of the information at the time of collection. Complaint specialists collect information directly from the individuals who are submitting the inquiry. Complaint specialists correct and update information in the inquiry at any time during the call if they become aware of any inaccurate information. Lastly, individuals may register for user accounts in the Citizens' Portal to review, amend, and augment previously submitted inquiries.

Privacy Risk: The EPIC system could maintain inaccurate information about constituents, particularly when the data is collected from other federal agencies in the event that the constituent corresponds with those agencies first.

Mitigation: FDIC sends acknowledgement letters to constituents making them aware that their complaint has been transferred to the FDIC. Constituents can now avail themselves to FDIC's redress procedures to access and amend incorrect information about them.

Privacy Risk: Information may be erroneously transposed, uploaded, or scanned into EPIC.

Mitigation: The accuracy of the data is checked at various stages of the complaint process. Additionally, should FDIC discover erroneous documents in a constituent's case files, FDIC will treat the incident as a breach and remediate it in accordance to the FDIC Breach Response Plan.

Use Limitation Risk:

Privacy Risk: FDIC could use the information for purposes other than that for which it was collected.

Mitigation: FDIC mitigates this privacy risk in several ways. First, FDIC limits the data collection in EPIC to only that which is required to process complaints/inquiries. Second, FDIC also limits access to EPIC to authorized users in four divisions based on their roles and responsibilities. Third, FDIC internal users receive informal training during onboarding. Reminders to protect PII are also given to FDIC internal users. Lastly, user manuals are provided to FDIC internal users to instruct them on how to use the EPIC system.

Privacy Risk: Due to the system's reliance on a commercial cloud service provider, there is a risk that the cloud service provider could potentially misuse the data.

Mitigation: Due to the encryption key management service within the CSP's cloud architecture, CSP personnel are incapable of using or redistributing any FDIC data processed and stored within EPIC. Should the CSP be required to access FDIC data to comply with federal law, or with a valid and binding order of a governmental or regulatory body, FDIC will provide the CSP with the necessary encryption keys to access the data. In the rare instances that CSP personnel have access to FDIC data because of a law enforcement requirement or court order, the CSP is obligated, by contract, to abide by all FDIC data protection requirements.

FDIC has access to the CSP's cloud hosting environment and may periodically audit the CSP to ensure information is protected in accordance with applicable contractual requirements. No additional mitigation actions are recommended.

Security Risks:

Privacy Risk: The volume and sensitivity of the data may make EPIC a target of potentially malicious actors.

Mitigation: The implementation of encryption, auditing protections, and the adherence to federal cyber security requirements mitigates this risk. FDIC uses industry-standard cybersecurity practices, including encryption of constituent data both in transit and at rest. Additionally, FDIC restricts access to constituent data to only those individuals with a demonstrated need to know in order to perform their official job functions.

Privacy Risk: The data maintained by the CSP for the purposes of cloud hosting may be vulnerable to breach because security controls may not meet system security levels required by FDIC.

Mitigation: The CSP is Federal Risk and Authorization Management Program (FedRAMP) approved, which means its cloud-based platform has undergone security assessments, authorization, and is continually monitored. FDIC is responsible for all PII associated within the EPIC system, whether on FDIC infrastructure or cloud infrastructure, and it therefore imposes strict requirements on the CSP for safeguarding PII data. Due

to the encryption key management service within EPIC's cloud architecture, CSP personnel is incapable of using or redistributing any FDIC data processed and stored within EPIC. The privacy of constituents is further protected by contractual language written in the CSP's contract requiring it to safeguard the FDIC PII data.

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?

PII collected as part of EPIC includes full name, address, telephone number, e-mail address, case number, and financial information, as it relates to the complaint submitted by the individual. Other PII could potentially be collected depending on what is submitted by the individual, however, only the information listed above is maintained for use in EPIC. All other information is identified by FDIC staff and removed before being entered into EPIC. Complaints and inquiries could contain extraneous PII. Any PII identified by FDIC staff that is not necessary to respond to the complaint are redacted prior to input into EPIC and/or deleted from EPIC upon discovery.

PII Element	Yes	No
Full Name	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Date of Birth	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Place of Birth	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Social Security Number	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Employment Status, History or Information	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Mother's Maiden Name	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Certificates (e.g., birth, death, naturalization, marriage, etc.)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Home Address	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Phone Number(s)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Email Address	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Employee Identification Number (EIN)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Driver's License/State Identification Number	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vehicle Identifiers (e.g., license plates)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Education Records	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Criminal Information	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Military Status and/or Records	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Investigation Report or Database	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Biometric Identifiers (e.g., fingerprint, voiceprint)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Photographic Identifiers (e.g., image, x-ray, video)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Other (Specify: _____)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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

Data Source	Description of Information Provided by Source
Constituents	Individuals or organizations who file complaints or inquiries via online forms, e-mail, fax, Community tools, and/or US postal mail delivery.
FDIC Personnel	FDIC personnel manually enter CRC and Call Center complaint data and upload any scanned documents/images sent via U.S.P.S. mail, email or fax associated with the complaint to EPIC; FDIC Department of Information Technology personnel enter FDIC internal users' full name in the EPIC system for account creation and management.
CALL Report Data from System of Uniform Reporting of Compliance and CRA Examinations (SOURCE) ⁴	CALL Report Data (from SOURCE System) provides basic bank asset information to EPIC regarding the bank identified by the constituent to EPIC.
Structure Information Management System (SIMS)	SIMS provides basic bank structure bank data to EPIC (e.g., Bank name, HQ address, asset size, web URL, FDIC Cert. number, etc).
FDICconnect (FCX)	FCX provides data to EPIC. Regulated banks, via FCX, can share responses to complaints, including PII information about constituents.

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

The EPIC system is operated in the Salesforce Cloud Service Providers (CSPs) government cloud. The Salesforce platform it operates in was Authorized to Operate by FDIC on October 25, 2017. Both are periodically reviewed as part of the FDIC Ongoing Authorization process. In May 2014, the CSP that provides the Salesforce platform achieved and has since maintained a FedRAMP Agency Authority to Operate (ATO) at the moderate impact level which was issued by U.S. Department of Health and Human Services (HHS).

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.

⁴ See System of Uniform Reporting of Compliance and CRA Exams PIA available at www.fdic.gov/privacy.

EPIC operates under the FDIC Privacy Act SORN 30-64-0005, Consumer Complaint and Inquiry Records (80 FR 66987), which covers correspondence and records of other communications between the FDIC and the individual submitting a complaint or making an inquiry, including copies of supporting documents and contact information supplied by the individual. This system may also contain regulatory and supervisory communications between the FDIC and the FDIC-insured depository institution in question and/or intra-agency or inter-agency memoranda or correspondence relevant to the complaint or inquiry.

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

No, the SORN does not require amendment or revision. Generally, the FDIC conducts review 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.

FDIC has publically posted a Privacy Act Statement before individuals access the EPIC system. Additionally, FDIC has implemented oral recitations of EPIC's Privacy Act Statement prior to the collection of any PII needed for inquiries.

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'.

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 contains policies and information related to SORNs, PIAs, FDIC's Privacy Policy, and contact information for the SAOP, the Privacy Program Manager, the Privacy Act System of Records (SOR) Clearance Officer, and the Privacy Program (Privacy@fdic.gov). The Protecting Privacy subpage discusses general practices related to the Privacy Act and PII. See <https://www.fdic.gov/about/privacy/protecting.html>.

Privacy Risk Analysis: Related to Transparency

Privacy Risk: Constituents, who erroneously submit complaints to FDIC, may not be aware that FDIC forwards their complaints to the appropriate financial regulator.

Mitigation: FDIC provides Privacy Act Statements to all constituents who submit complaints directly. The Privacy Act Statements inform constituents that FDIC may furnish their complaint "to the Federal or State supervisory authority that has direct supervision over the financial institution."

Privacy Risk: Constituents, who submit their inquiries telephonically, may be not given Privacy Act Statements and therefore unaware of FDIC's uses of their PII.

Mitigation: This is no longer a risk. FDIC has implemented oral recitations of EPIC's Privacy Act Statement prior to the collection of any PII needed for inquiries. Additionally, this PIA and the SORN listed in Section 2.2 serves as notice of the FDIC's uses of PII received from constituents.

Privacy Risk: Constituents, whose complaints are referred from other financial regulators may be unaware of FDIC's uses of their PII.

Mitigation: Other financial regulators provide constituents notice that their complaint is shared with other financial regulators for enforcement and statutory purposes. Once FDIC receives the complaint, FDIC sends the constituent an acknowledgement email/letter informing the individual of the complaint referral.

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?

Individuals are able to access their information by registering for a user account and logging into the Citizens' Portal. After logging into the portal, individuals have the ability to make changes to their information.

Additionally, 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 1031.1. Access procedures for this information system or project 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 1360.1. 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.

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

Individuals are able to access their information by registering for a user account and logging into the Citizens' Portal. After logging into the portal, individuals have the ability to make changes to their information.

Additionally, 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 Section 2.2 of this PIA.

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

After logging into the Citizens' Portal, individuals have the ability to review and make changes to the information they have previously submitted. Additionally, 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 1031.1.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: The personnel of financial institutions responding to complaints referred by FDIC cannot correct or amend inaccurate information about them contained in EPIC.

Mitigation: The PII of financial institution personnel contained in EPIC is limited to basic contact information such as name, telephone number, and email address. The FDIC does not use these individuals' PII to deprive them of a right or benefit. Financial institution personnel voluntarily include their PII in responses to FDIC for contact purposes.

Privacy Risk: Constituents may not be able to have their complaint resolved after they have corrected inaccurate information in EPIC because FDIC has already sent the complaint to the relevant financial

institution and that financial institution cannot retrieve information on the individual as a result of the inaccurate information.

Mitigation: Once FDIC submits a complaint to a bank, it does not provide the bank with updated information related to that complaint. However, financial institutions notify FDIC when they cannot retrieve information on constituents based on the information provided. An FDIC complaint specialist then writes a personalized letter to the constituent noting that there may have been updated information that was not sent to the financial institution. The FDIC complaint specialist also requests the constituent review and update any inaccurate information submitted in the initial complaint. Once constituents provide FDIC with updated information, FDIC creates an additional complaint in EPIC, links it to the initial complaint, and sends both complaints to the relevant bank for resolution.

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 1360.19). PIAs are posted on FDIC's public-facing website, <https://www.fdic.gov/about/privacy/index.html>.

4.4 What roles, responsibilities and access will a contractor have with the design and maintenance of the information system or project?

Contractors will assist FDIC with integrating EPIC into the CSP's platform. Contractors will have access to PII to build and support the EPIC solution to meet FDIC specifications.

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.

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.

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?

There are profiles and roles that are created which provide both internal and external users with only the necessary information needed to complete their jobs. These profiles dictate which attributes they are able to view and/or edit. The data owner of each system must also approve ARCS requests for each individual with appropriate access to the data based on their job responsibility. Furthermore, FDIC internal users can only access the CSP environment from an FDIC network, and FDIC users also undergo annual PII and data security training.

Additionally, the two-factor authentication is in place to protect external users (constituents and financial institutions) while logging into both the Citizens' and Bankers' Portals. Whenever a user registers or logs in, a randomly-generated token is created and submitted to the user via email.

Moreover, 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. Lastly, 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 FDIC Circular 1031.1. Disclosures are tracked and managed using FOIAExpress.

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 1031.1.

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 1031.1.

Privacy Risk Analysis: Related to Accountability

Privacy Risk: Constituents are not able to appeal unfavorable resolutions of complaints.

Mitigation: FDIC's statutory mandate is to promote and enforce compliance by FDIC supervised financial institutions with federal consumer protection laws, including those relating to fair lending and unfair and deceptive practices. FDIC carries out this mission by (1) investigating constituent complaints involving financial institutions it supervises; and (2) responding to inquiries from the public and financial institutions about consumer protection and fair lending matters. FDIC's scope of authority does not ordinarily extend to the resolution of complaints involving factual disputes or contractual matters, or matters that have been or are in the process of being litigated.

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:

Section 9 of the Federal Deposit Insurance Act (12 U.S.C. 1819) and Section 202(f) of Title II of the Federal Trade Improvement Act (15 U.S.C. 57a(f)).

Privacy Risk Analysis: Related to Authority

Privacy Risk: FDIC may investigate complaints where it has no legal authority to do so.

Mitigation: FDIC staff reviews complaints to determine if they are in the scope of the FDIC's legal authority. Should FDIC determine that the complaint is not in the scope of its authority, FDIC staff will forward the complaint to the appropriate regulatory authority.

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?

The constituents have the capability to upload and include any information in their complaints. However, FDIC staff will remove/redact any PII irrelevant PII. The only PII that EPIC maintains is the PII specified in Question 1.2.

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.

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?

The information stored in EPIC is retained for the greater of five years or two years after the last activity on the file in accordance with the FDIC's Records Retention and Disposition Schedule SUP7000.

Hardcopy documents are maintained while the complaint is open for reference purposes, and are shredded after the complaint is closed. The shredding is generally completed within 60 days, except for Fair Lending cases, which may take up to 180 days.

There is no retention by the CSP, as it does not have access to any FDIC data.

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 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 information stored in EPIC is retained for the greater of five years or two years after the last activity on the file in accordance with the FDIC's Records Retention and Disposition Schedule SUP7000.

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?

Use of sensitive data outside the production environment requires management approval via a waiver. Any production data, including PII, may not be used outside of the production environment unless a waiver has been approved by management, and appropriate controls have been put in place.

Privacy Risk Analysis: Related to Minimization

Privacy Risk: More information may be collected than is necessary to resolve an inquiry or complaint.

Mitigation: FDIC limits the scope of information collected in EPIC to the amount of data necessary to act upon the complaints filed. Although the system stores PII provided in the complaint, this information is captured only where it is relevant to the resolution. Any PII identified by FDIC staff as not necessary to respond to the complaint is redacted prior to input into EPIC and/or deleted from EPIC upon discovery.

Privacy Risk: FDIC may retain information longer than necessary.

Mitigation: FDIC retains information contained in EPIC in accordance with its established retention schedule. FDIC divisions are responsible for deleting or archiving information in accordance with the retention schedules. This risk is mitigated because FDIC follows all pertinent records schedules discussed in sections 6.2 and 6.4. In addition, the FDIC Records and Information Management Section provides trainings to inform FDIC programs of proper record retention, disposition requirements, records inventory training, file plan training, and file structure training to ensure that FDIC personnel are aware of all records requirements.

Privacy Risk: The EPIC system may retain un-submitted or incomplete complaints in perpetuity.

Mitigation: For un-submitted complaints, EPIC does not retain data. No data is captured in EPIC until complaints have been submitted. Incomplete complaints, complaints that lack sufficient information for resolution, are retained in accordance with the EPIC retention schedule. FDIC notifies constituents in writing and informs them there is not enough information to investigate the complaint. FDIC then closes out the complaint. Should constituents provide additional information in support of their complaint, the FDIC will create a new complaint in EPIC, link the previous complaint, and forward to the relevant financial institution for resolution.

Privacy Risk: Due to the storage of data on a commercial cloud platform, there could be a failure to adhere to FDIC retention guidelines and schedules.

Mitigation: During the period that the contract with the EPIC CSP is active, the FDIC has direct access to the data and ensures that appropriate retention schedules are followed. After the contract period ends, the CSP is required to adhere to the retention restrictions specified in the contract. Due to the encryption key management service within EPIC's cloud architecture, CSP personnel are incapable of using or redistributing any FDIC data processed and stored within EPIC. Should the CSP be required to access FDIC data to comply with federal law, or with a valid and binding order of a governmental or regulatory body, FDIC will provide the CSP with the necessary encryption keys to access the data. In the rare instances that CSP personnel has access to FDIC data because of a law enforcement requirement or court order, the CSP is obligated, by contract, to abide by all FDIC record retention schedules and privacy/security requirements.

FDIC has access to CSP's cloud hosting environment and may periodically audit the vendor to ensure information is retained per the applicable retention schedules. No additional mitigation actions are recommended.

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?

Generally, the EPIC system collects PII directly from individuals. Individuals file complaints or inquiries themselves and provide their own information. However, some complaints are referred to FDIC by other federal and state financial regulators. 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.

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 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: When inquiries are made telephonically, FDIC employees rather than the individuals themselves perform data entry of inquiring individuals' information and this may result in inaccurate information.

Mitigation: Complaint specialists verify the accuracy of the information at the time of collection. Complaint specialists collect information directly from the individuals who are submitting the inquiry. Complaint specialists correct and update information in the inquiry at any time during the call if they become aware of any inaccurate information. Lastly, individuals may register for user accounts in the Citizens' Portal to review, amend, and augment previously submitted inquiries.

Privacy Risk: The EPIC system could maintain inaccurate information about constituents, particularly when the data is collected from other federal agencies in the event that the constituent corresponds with those agencies first.

Mitigation: FDIC sends acknowledgement letters to constituents making them aware that their complaint has been transferred to the FDIC. Constituents can now avail themselves to FDIC's redress procedures to access and amend incorrect information about them.

Privacy Risk: Information may be erroneously transposed, uploaded, or scanned into EPIC.

Mitigation: The accuracy of the data is checked at various stages of the complaint process. Additionally, should FDIC discover erroneous documents in a constituent's case files, FDIC will treat the incident as a breach and remediate it in accordance to the FDIC Breach Response Plan.

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.

EPIC generally collects information directly from the individual and 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.

EPIC also receives a minimal number of complaints from federal financial regulators. The FDIC does not have the ability to provide Privacy Act Statements or privacy notices prior to the Agency's processing of individuals' PII. Constituents should review the referral agency's privacy notices.

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.

EPIC generally collects information directly from the individual, it describes in the Privacy Act Statement and other privacy notices the choices available to the individual and obtains consent with respect to the collection, use, and disclosure of PII.

EPIC also receives a minimal number of complaints from federal financial regulators. The FDIC does not have the ability to provide Privacy Act Statements or privacy notices prior to the Agency's processing of individuals' PII. Constituents should review the referral agency's privacy notices.

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.

8.3 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/about/privacy/index.html>, instructs viewers 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 privacy risks associated with Individual Participation for EPIC.

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, and stores PII, consisting of basic contact and financial information, to respond to, track, and resolve complaints and inquiries received from the public and financial institutions. This PII is also used to create user accounts in the Communities and Banker's Portals. Any extraneous PII is redacted by complaint specialists.

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.

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

FDIC Internal Users

Authorized users in the Division of Consumer and Depositor Protection (DCP), Division of Insurance and Research (DIR), Division of Administration (DOA), and the Office of the Ombudsman (OO) have access to this data. Complaint specialists of DCP, DIR, DOA, and OO are responsible for the review and resolution of complaints and inquiries. All FDIC internal users of EPIC are requested and approved through FDIC Access Request and Certification System⁵ (ARCS) system.

Constituents

Constituents have access to EPIC via the Citizens' Portal. When individuals register for the portal for the first-time, they are prompted to provide their first name, last name, and their email address. Individuals enter those details and users receive an email to confirm their registration. Once users have confirmed their registration, they are prompted to enter a random token which is provided to them via email.

State Financial Regulators

State financial regulators have access through EPIC through the Extranet and Bankers' Portal. EPIC is integrated with FDIC Extranet to allow one way communication from EPIC to state banking regulators. Once an MOU is executed, FDIC share complaints to state financial regulators about financial institutions in their respective states. State financial regulators are allowed to access the Bankers' Portal and only see a summary view of the closed complaints for their states' financial institutions but no complaint details.

Financial Institutions

Financial institutions gain access to EPIC via the Bankers' Portal. To gain access to the Bankers' Portal, financial institutions will continue to be authenticated by FCX. The financial institutions are then routed from FCX to the Bankers' Portal. Financial institutions can only access their own complaints/inquiries through the Bankers' Portal. All U.S. financial institutions have certification numbers issued by the FDIC. The FDIC certification number is unique to each bank. Users of the Bankers' Portal are provisioned based on their bank's certification number. EPIC, through the Bankers' Portal, only allows financial institutions to respond to their own complaints/inquiries.

⁵ See Access and Request Certification System PIA available at www.fdic.gov/privacy.

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.

Data Gathering Tool: EPIC shares data to the Data Gathering Tool (DGT) to provide complaint information to bank examination staff. This allows bank examination staff to have a general idea of the volume/type of complaints against a bank when an examination commences.

Microsoft Outlook 365: EPIC is integrated to Microsoft Outlook 365. FDIC internal users of EPIC send an "FDIC basic acknowledgment" email to constituents upon receipt of the complaint or inquiry. EPIC will share the constituent's email address with Outlook for this purpose. Additionally, Outlook is used to communicate with external banking agencies about a complaint, secured via Zix Mail.

Quarterly Compliance Risk Profile Tool: EPIC users provide data and reports (manually) that are then incorporated into DCP's Quarterly Compliance Risk Profile Tool. This is high level summary data (volume of complaints per bank, etc.).

System of Uniform Reporting of Compliance and CRA Examinations (SOURCE): SOURCE system provides basic asset information to EPIC regarding financial institutions identified by the constituent to EPIC.

Structure Information Management System (SIMS): SIMS provides basic bank structure data to EPIC (e.g., Bank names, address, asset size, web URL, FDIC Certification Number, etc.).

FDICconnect (FCX): The FCX system authenticates regulated financial institutions to allow access to the Bankers' Portal.

FDIC Extranet: The FDIC Extranet provisions and authenticates state regulators in order for these entities to gain read access to the Bankers' Portal.

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 FDIC 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.

EPIC shares PII externally with the following types of entities:

Financial Institutions: EPIC, through the Bankers' portal, may share complaint/inquiry correspondence with federally regulated financial institutions. This sharing may include any of the PII that was specified in Section 1.2.

Federal Financial Regulators: EPIC, through Microsoft Outlook 365, may share complaint/inquiry correspondence with other financial regulatory agencies (e.g., the Federal Reserve, Consumer Financial Protection Bureau, and the Office of the Comptroller of the Currency). This may include any of the PII that was specified in Section 1.2. If a constituent's incoming correspondence is sent to another federal regulatory agency for handling, the constituent is sent a letter notifying them of the referral and providing them the name and address of the agency.

State Financial Regulators: EPIC, through the Bankers' Portal, may share complaint/inquiry correspondence with state banking authorities. A MOU is executed before access is granted to the Bankers' Portal. This sharing may include any of the PII that was specified in Section 1.2.

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 1031.1 '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: FDIC could use the information for purposes other than that for which it was collected.

Mitigation: FDIC mitigates this privacy risk in several ways. First, FDIC limits the data collection in EPIC to only that which is required to process complaints/inquiries. Second, FDIC also limits access to EPIC to authorized users in four divisions based on their roles and responsibilities. Third, FDIC internal users receive informal training during onboarding. Reminders to protect PII are also given to FDIC internal users. Lastly, user manuals are provided to FDIC internal users to instruct them on how to use the EPIC system.

Privacy Risk: Due to the system's reliance on a commercial cloud service provider, there is a risk that the cloud service provider could potentially misuse the data.

Mitigation: Due to the encryption key management service within the CSP's cloud architecture, CSP personnel are incapable of using or redistributing any FDIC data processed and stored within EPIC. Should the CSP be required to access FDIC data to comply with federal law, or with a valid and binding order of a governmental or regulatory body, FDIC will provide the CSP with the necessary encryption keys to access the data. In the rare instances that CSP personnel have access to FDIC data because of a law enforcement requirement or court order, the CSP is obligated, by contract, to abide by all FDIC data protection requirements.

FDIC has access to the CSP's cloud hosting environment and may periodically audit the CSP to ensure information is protected in accordance with applicable contractual requirements. No additional mitigation actions are recommended.

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: The volume and sensitivity of the data may make EPIC a target of potentially malicious actors.

Mitigation: The implementation of encryption, auditing protections, and the adherence to federal cyber security requirements mitigates this risk. FDIC uses industry-standard cybersecurity practices, including encryption of constituent data both in transit and at rest. Additionally, FDIC restricts access to constituent data to only those individuals with a demonstrated need to know in order to perform their official job functions.

Privacy Risk: The data maintained by the CSP for the purposes of cloud hosting may be vulnerable to breach because security controls may not meet system security levels required by FDIC.

Mitigation: The CSP is Federal Risk and Authorization Management Program (FedRAMP) approved, which means its cloud-based platform has undergone security assessments, authorization, and is continually monitored. FDIC is responsible for all PII associated within the EPIC system, whether on FDIC infrastructure or cloud infrastructure, and it therefore imposes strict requirements on the CSP for safeguarding PII data. Due to the encryption key management service within EPIC's cloud architecture, CSP personnel is incapable of using or redistributing any FDIC data processed and stored within EPIC. The privacy of constituents is further protected by contractual language written in the CSP's contract requiring it to safeguard the FDIC PII data.