FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Threshold Analysis (PTA) and/or Privacy Impact Assessment (PIA)

for

Division of Insurance Research (DIR) use of

Enterprise Public Inquiry and Complaints (EPIC) on the Salesforce Platform

Date Approved by Chief Privacy Officer (CPO)/Designee: 9/20/2018

PTA/PIA TEMPLATE VERSION 1.9 – August 2017

SECTION I – OUTSOURCED INFORMATION SERVICE DESCRIPTION

1. Describe the outsourced service and its purpose.

The Enterprise Public Inquiry and Complaints (EPIC) effort is an enterprise Software as a Service (SaaS) solution that is built on the Salesforce platform. It is a configured solution to manage public and banker complaints and inquiries received by the Federal Deposit Insurance Corporation (FDIC). EPIC is an automated, online system that enables staff within the Division of Insurance (DIR) to add, update, review, and report on individual cases of consumer and financial institution questions, suggestions and requests about DIR data and publications. The methods of communication to be managed within EPIC include complaints and inquiries received via telephone, email, web-forms. While DCP EPIC users receive material by mail or fax, DIR does not receive material by mail or fax.

EPIC captures regular and controlled correspondence and telephone calls from consumers and financial institutions that are not examination related. EPIC is a nationwide system that is accessible from FDIC's Washington, Regional, and Field Offices. In addition to full data entry capabilities, users can print reports based on user-specified criteria, attach scanned documents to specific records, and automatically generate reply letters. DIR does not capture any controlled correspondence. Controlled correspondence includes items from the Chairman's Office, President, and Congressional staff. All items of that nature are routed through the Office of Legislative Affairs (OLA) to DCP.

The solution will be acquired and delivered in phases. The initial 2017 scope of work involved the replacement of two legacy systems used for two communication and inquiry tracking systems:

-Office of the Ombudsman's Communication Tracking System - Ombudsman Automated Tracking System (CTS-OATS); and

-DCP's Specialized Tracking and Reporting System (STARS).

EPIC is now replacing DIR's Customer Communication and Tracking System (CCATS).

SECTION II – DATA TYPE, SOURCES, AND USE

2. Describe all information/data that will be collected, used, maintained or generated by the Outsourced Provider (Vendor) as part of the services provided under the contract. If no information/data is involved, select Not Applicable.

DIR in EPIC

FDIC receives, responds to, tracks and reports on inquiries received from the public and bankers. DIR will need to be able to store information related to the communications and report to a variety of constituencies on the complaints and inquiries they receive and process. Hence, all communications made to the FDIC by the customer(s) has to be tracked within the EPIC system. The customer(s) who contacts FDIC are Consumer, Academia, Banker, Analyst, Congress/Senate/White House, Media/Press, Attorney, Professionals, FDIC-Management, FDIC-Employee, and other Federal, State and Local Agencies.

PII will be collected and retained in a variety of ways; DIR's online"Questions, Suggestions & Requests" form is similar to (http://www2.fdic.gov/idasp/DIRSInfoRequest.asp). The form collects: requestor type (e.g., academic, banker, consumer), name, email address, phone/fax numbers, title, organization name, state, and question. Also, if applicable, the form collects previously contacted FDIC information and the financial institution's name, city, state and FDIC Certificate number Only name, email address and the requestor's question are mandatory as they are deemed necessary to answer the request. The other fields are optional and are collected in order to better serve the requestor. This form will be replaced by a Salesforce online form, but will largely capture the same type of information.

EPIC does not have any fixed database fields to record highly sensitive PII (SSN, personal bank account or financial information, date of birth, etc.). Social security numbers (SSN) or any other single item of information that may be considered sensitive PII are never required or requested by DIR. While requestors are never normally asked to submit this type of PII, it is possible that a requestor may inadvertantly submit such information in correspondence sent to DIR for the FDIC by email or webform.

DIR has not recieved a question via mail or fax in 5 plus years. However, if DIR does receive such a request (with or without sensitive PII) via mail or fax, the EPIC record in question would be routed to the Division of Depositor and Consumer Protection (DCP) within EPIC or the Division of Resolutions and Receiverships (DRR), outside of EPIC. DRR is not a user of EPIC. Additional information, such as home address, may be provided voluntarily in cases involving a requestor electing to continue communication with FDIC through United States Postal Service (USPS) mail rather than email.

EPIC contains the requestor's incoming correspondence, internal codes to identify the requestor's concerns, information concerning the bank in question (bank name, address, class code, supervisory region), and internal tracking dates regarding action(s) taken on the record.

EPIC contains consumer correspondence that may have been referred from another federal regulatory agency. For example, if a consumer writes to the Office of the Comptroller of the Currency (OCC) about a financial institution supervised by FDIC, the OCC would forward the incoming consumer correspondence to the FDIC for handling and responding.

DIR use of EPIC is focused on answering questions about the industry analysis publications and data that DIR maintains on the FDIC website. DIR does not tranfer or forward cases outside of FDIC. DIR will answer the consumer's inquiry, direct them to the proper agency, and close out the case.

EPIC will also store FDIC employee names to assign user profiles (giving some administrative access and others standard user access) in EPIC. This is to allow FDIC to manage which EPIC users are managing which requests. EPIC does not have any fixed database fields to record PII (SSN, personal bank account or financial information, date of birth, etc.) While correspondents with FDIC DIR are never asked to submit this PII, there is no way to prevent a submitter from including any type of data in the correspondence. Any additional PII that is identified as not necessary to respond to the request (not one of the identified PII elements in question 4) will be redacted prior to input into EPIC and/or deleted from EPIC upon discovery.

3. Describe the intended purpose and use of the above information/data. If no information/data is involved, select Not Applicable.

The categories of customers who may contact DIR are: Consumer, Academia, Banker, Analyst, Congress/Senate/White House, Media/Press, Attorney, Professionals, FDIC-Management, FDIC-Employee, and other Federal, State and Local Agencies. The PII collected is both relevant and necessary for the purpose for which it was designed. This is part of the system design and is documented in the EPIC user manual. Data can be retrieved by the requestor's name, address, email address, or telephone number. However, information is typically retrieved by EPIC record/case number. Management reports are used to monitor workflows or timeliness. Authorized users may access reports and distribute them to internal, first-line supervisors. Supervisory records are kept logically separated in the EPIC solution.

4. What types of personally identifiable information (PII) are (or may be) included in the information specified above? The only PII that EPIC maintains for DIR is the full name of the DIR user and the PII specified below that may be provided by the requestor. Any of the following items may be inadvertently received through open text fields in the online comment form or included by the requestor in their submission, but, when identified by DIR as unnecessary, will be removed by DIR staff.

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

5. If Social Security Number (SSN) is checked in question 4, please answer the following:

a) Explain the business purpose requiring the collection of SSNs: Collection of SSN is not required, however, a requestor of information could include SSN within a text box.

b) Provide the legal authority which permits the collection of SSNs. Collection of SSN is not required, however, a requestor of information could include SSN within a text box.

c) Identify whether the SSN is masked or otherwise truncated as part of the outsourced service: Collection of SSN is not required, however, a requestor of information could include SSN within a text box.

6a. Please provide an estimate of the number of records maintained by the vendor for this contract that contain PII:

Estimated Number of Records Containing PII				
0 ☐	1-500 ☐	501-1,000 ☐	1,001 – 2,500 ☐	2,501 – 5,000 ☐
5,001 – 7,500 ☐	7,501 – 10,000 ☒	10,000 – 50,000 ☐	50,000 – 100,000 ☐	over 100,000 ☐

6b. If "0" was answered for 6a, please explain[1]: N/A

7. What are the sources of data (both PII *and* non-PII) for the outsourced service/project? How is the data derived?

Data Source[2] (List all sources that the Outsourced Provider collects, obtains or receives data from, as part of the services provided under the contract.)	**Type of Data Provided by Source & How It is Derived** (Describe the type of PII and non-PII data provided by each source. If PII is included in the data, list the specific PII elements, and explain how the PII is derived.)	**Does Data Include PII?**
FDIC DIR Web Form and FDIC Call Center	Individuals calling the FDIC about an inquiry will speak with DOA, who may route the call to DIR, who may collect PII so EPIC users can correspond with the individual. This may include any of the PII specified in question 4.	☒ Yes ☐ No
Email	Individuals who send email about a complaint or inquiry may send any of the PII specified in question 4.	☒ Yes ☐ No
Routing Within EPIC from DCP or DOA	If a DCP or DOA user receives a case in EPIC that should be processed by DIR, that case will be routed to DIR. However, only the case information that DIR needs to process the case will be forwarded to DIR.	☒ Yes ☐ No
FDIC Personnel	DIR personnel will manually enter DIR inquiry data and any	☒ Yes ☐ No

[1] If the vendor has not received work to date for this contract and "0" is checked in 6a, please explain approximately how many records may be maintained by the vendor if they are awarded work under this contract in the future. Additionally, the Division responsible for this vendor must update this PIA to reflect the accurate number of records containing PII that the vendor maintains if this changes in the future.[2] Examples of potential data sources include, but are not limited to: internal (FDIC) or external (non-FDIC) systems, websites, individual members of the public (e.g., customers, borrowers, etc.), FDIC employees, FDIC contractors, credit bureaus, commercial entities, public records, government agencies, etc.

[2] Examples of potential data sources include, but are not limited to: internal (FDIC) or external (non-FDIC) systems, websites, individual members of the public (e.g., customers, borrowers, etc.), FDIC employees, FDIC contractors, credit bureaus, commercial entities, public records, government agencies, etc.

	scanned documents/images, sent email, or information associated with the inquiry to EPIC; When a new FDIC EPIC user needs to be added to EPIC, DIT personnel will enter DIR 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)	CALL Report Data (from SOURCE System) provides basic bank asset information to EPIC (regarding the bank identified by the requestor to EPIC).	☒ Yes ☒ No
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).	☒ Yes ☐ No
FDICConnect (FCX)	FCX provides data to EPIC. Regulated banks, via FCX, can share responses to requests, including PII information about requests (which include any/all of the PII from question 4).	☒ Yes ☒ No
Avaya	Computer-telephony integration, in support of the Central Call Center operations. Avaya will auto populate the caller's phone number into EPIC.	☐ Yes ☒ No
Zip Info	FDIC currently obtains zip code information from a third party web site known as (Zipinfo) for maintaining accurate address information in various tracking systems.	☐ Yes ☒ No

8. How will FDIC and/or the Outsourced Service Provider retrieve data or records as part of the outsourced service or project? Can data be retrieved using a personal identifier (e.g., name, address, SSN, EIN, or other unique identifier)?

Yes, data can be retrieved by a personal identifier – complainant's name, address, email address, or telephone number. However, information is typically retrieved by EPIC record/case number.

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

EPIC operates under the FDIC Privacy Act SORN 30-64-0005, *Consumer Complaint and Inquiry Records* (80 FR 66987).

This completes the PTA.

- Do not complete the rest of the form, if the service provider is not processing or maintaining sensitive PII. This is the case, if you checked:
  - NOT APPLICABLE for question 3 and NO for all items in question 4; OR
  - Only Full Name in question 4.

- Continue completing the remainder of the form, i.e., Sections III thru VI in their entirety (questions 10 through 18), if the service provider is processing or maintaining sensitive PII. This is the case, if you checked:
  - YES for Social Security Number (SSN) in question 4; OR
  - YES for SSN or for Full Name in addition to one or more boxes in question 4.

- If you have questions or are unsure about whether or not you should complete the remainder of this form, please contact your Division ISM or the Privacy Program Office (privacy@fdic.gov).

SECTION III – DATA ACCESS AND SHARING

10. In the table below, specify the systems/applications and parties (FDIC and non-FDIC) that the Outsourced Service Provider will share or provide PII data to as part of the outsourced service.

PII Will Be Accessed By and/or Provided To:	Yes	No	If Yes, Explain How and Why the PII Will Be Accessed/Shared
10a. FDIC Outsourced Service Provider (OSP) Staff; OSP Subcontractors; and/or OSP Systems	☐	☒	N/A – no Salesforce staff will have access to any PII contained within EPIC.
10b. FDIC Personnel and/or FDIC Systems/ Applications	☒	☐	PERSONNEL DCP, DIR, OO and DOA employees will have access to the PII within EPIC in the course of their work (while managing cases and communicating within EPIC). DIT will have administrative access. This may include some or all of the PII specified in question 4. SYSTEMS EPIC shares data to the Data Gathering Tool (DGT) to provide complaint information to bank examination staff (DCP). This allows bank examination staff to have a general idea of the volume/type of complaints against a bank when an examination commences. EPIC is integrated to Microsoft Outlook 365. DCP users of EPIC send an "FDIC basic acknowledgment" email to complainants upon receipt of the complaint or inquiry. EPIC will share the complainant'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. EPIC is integrated to the Extranet (to allow one way communication from EPIC to State Banking Authorities); DCP users of EPIC, once an MOU is executed, share complaints about the financial institutions regulated by the respective states. EPIC could share PII of complainants (which include any/all of the PII from question 4). EPIC is integrated with FCX (to allow 2 way communication with regulated banks). DCP users of EPIC share complaints to regulated banks, including PII of complainants (which include any/all of the PII from question 4). 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.). Zipinfo-zip code validation Avaya-telephony integration FDIC Contractors supporting EPIC FDIC Salesforce Integrator support contractors will have access to PII within EPIC to build and support the EPIC solution to meet FDIC specifications. DOA contractors operate the FDIC call center.
10c. Individual Members of the Public (e.g., bidders, investors, borrowers, customers, etc.)	☐	☒	N/A – no members of the public will have access to any PII contained within EPIC.
10d. Other Non-FDIC Entities/ Parties and/or Non-FDIC Systems/Applications	☒	☐	EPIC, through FDICconnect, may share complaint/inquiry correspondence with federally regulated banks. This may include any of the PII that was specified in question 4.
10e. Federal, State, and/or Local Agencies	☒	☐	EPIC, through Outlook (secured by Zix), 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 question 4. If a consumer's incoming correspondence is sent to another federal regulatory agency for handling, the consumer is sent a letter notifying them of the referral and providing them the name and address of the agency. EPIC, through the Extranet, may share complaint/inquiry correspondence with state banking authorities. This may include any of the PII that was specified in question 4.
10f. Other	☐	☒	N/A

11. If data will be provided to, shared with, or maintained by non-FDIC entities (such as government agencies, contractors, or Outsourced Information Service Providers), have any of the following agreements been issued?

Data Protection and/or Sharing Agreements	Yes	No
FDIC Confidentiality Agreement (Corporation) (Cap Gemini, Coresphere)	☒	☐
FDIC Confidentiality Agreement (Individual)	☒	☐
Non-Disclosure Agreement (NDA)	☐	☒
Memoranda of Understanding (MOU)	☐	☒
Information Sharing Agreements (ISA)	☐	☒
Authentication Risk Assessment	☐	☒

Other Applicable Agreement(s) (*Specify*: _____)	☐	☐
If you answered NO to any item above, please provide additional information if available: _____		

SECTION IV – NOTICE AND CONSENT

12. Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

☐ No. Individuals do not have the opportunity to "opt out" of providing their data and/or consenting to particular uses of their information.

☒ Yes. Individuals have the opportunity to decline to provide their personal data or to consent to particular uses of their information.

Customers initiate contact with FDIC by submitting either inquiries, requests, complaints (regarding financial institutions), and/or suggestions. At any point during this process, the customer can choose to remain anonymous and opt-out of providing any PII. However, if they would like to receive a written response from the FDIC, they must provide the necessary PII so that FDIC may mail/email them a response.

13. If PII is being collected via a public-facing website and/or application as part of this outsourced service, has the Outsourced Information Service Provider posted any of the following types of privacy policies or Privacy Act notices?

☐ No
☒ Yes *(If yes, check applicable box(es) below.)*
- ☒ Link to FDIC Privacy Policy
- ☒ FDIC Privacy Act Statement
- ☒ Contractor Privacy Policy or Statement
- ☐ No Privacy Policy has been posted

SECTION V – DATA SECURITY AND ACCURACY

14. Please assert what administrative procedures and technical safeguards are in place to protect sensitive PII data in the Outsourced Information Service Provider's care.

☐ [Outsourced Information Service Provider name] [has gone/will go] through the security review required by the FDIC's Outsourced Information Service Provider Assessment Methodology to determine and/or verify their having appropriate physical, technical, and administrative security measures to safeguard FDIC-provided PII and other sensitive data. If it has gone through the Methodology, has it been approved? ☐ NO ☐ YES

☒ The FDIC conducts background investigations (BIs) on key Salesforce personnel and other applicable personnel prior to their beginning work on the contract.

☒ Salesforce is subject to periodic compliance reviews by FDIC. Per the contract, scheduled and unannounced inspections and assessments of the Outsourced Service Provider's facilities, personnel, hardware, software and its security and privacy practices by either the FDIC information technology staff, the FDIC Inspector General, or the U.S. General

Accountability Office (GAO). These inspections may be conducted either by phone, electronically or in-person, on both a pre-award basis and throughout the term of the contract or task order, to ensure and verify compliance with FDIC IT security and privacy requirements, as per the FedRamp Package.

☒ Other (Explain any other administrative and/or technical safeguards in place to protect PII data in the Outsourced Information Service Provider's care.) ***Attach the Contract Clause Verification Checklist to the back of this form.***

Appropos to FedRamp-certified PaaS solutions, Salesforce has not gone through the FDIC Information Service Provider Assessment Methodology. Salesforce has gone through the FedRamp Certification process. FDIC has reviewed this package. The Salesforce Platform is going through the FDIC ATO process.
See also, https://www.salesforce.com/company/privacy/.

EPIC user account creation and deletion requests go through the FDIC standard access control procedures, which require management approval, as well as setting up the internal user profiles through the applications administrative table. Users' rights are limited by role. Users only have access to EPIC data pertaining to records they are authorized to access (for example, those with access to telephone records only, do not have access to stored images of correspondence).

Complaint and inquiry data is available to other federal regulatory agencies upon request. These requests may involve the volume of complaints and inquiries that were received for a specific timeframe, or may be based on the subject of the complaint/inquiry, (ie., number of credit card complaints received). Senior Management determines the criteria for the type of data shared and no agreements have been effected.

Authorized users are responsible for properly using the data and are accountable if the data is compromised.

15. What are the procedure(s) for ensuring that the information maintained is accurate, complete and up-to-date?

☒ Data is collected directly from individuals. As such, the FDIC and its vendors rely on the individuals to provide accurate data.

☐ The vendor/contractor works with FDIC to verify the integrity of the data [before, in conjunction with, and/or after] inputting it into the system or using it to support the project.

☒ As necessary, an authorized user of EPIC checks the data for completeness by reviewing the information, verifying whether or not certain documents or data is missing, and as feasible, updating this data when required.

☒ Other (*Please explain*.)

Data-integrity checks are completed against required fields to ensure FDIC has the data needed to provide a response back to the complainant.

16. In terms of assuring proper use of the data, please assert whether the following statements are true for the Outsourced Information Service Provider.

☒Within FDIC, the Enterprise Public Inquiry and Complaints (EPIC) Program Manager/Data Owner, Technical Monitors, Oversight Manager, and Information Security Manager (ISM) are collectively responsible for assuring proper use of the data. In addition, it is every FDIC user's responsibility to abide by FDIC data protection rules which are outlined in the FDIC's Information Security and Privacy Awareness training course which all employees take annually and certify that they will abide by the corporation's Rules of Behavior for data protection.

☒ Additionally, the Outsourced Information Service Provider is responsible for assuring proper use of the data. Policies and procedures have been established to delineate this responsibility, and the vendor has designated personnel to have overall accountability for ensuring the proper handling of data by vendor personnel who have access to the data. All vendor personnel with access to the data are responsible for protecting privacy and abiding by the terms of their FDIC Confidentiality and Non-Disclosure Agreements, as well as the vendor's corporate policies for data protection. Access to certain data may be limited, depending on the nature and type of data.

See this link for details:

https://www.salesforce.com/company/privacy/

☒ The Outsourced Provider must comply with the Incident Response and Incident Monitoring contractual requirement.

☐ None of the above. *(Explain why no FDIC staff or Outsourced Information Service Provider personnel have been designated responsibility for assuring proper use of the data.)*

SECTION VI – DATA RETENTION AND DISPOSAL

17. Where will the Outsourced Service Provider store or maintain the PII data identified in question 4? Describe both electronic and physical storage repositories, as applicable.

The EPIC system is only operated in the Salesforce Gov Cloud. In May 2014, Salesforce achieved and has since maintained a FedRAMP Agency Authority to Operate (ATO) at the moderate impact level issued by U.S. Department of Health and Human Services (HHS) for the Salesforce Government Cloud.

18. Specify the period of time that data is retained by the Outsourced Service Provider and the specific procedures for disposing of or returning the data at the end of the retention period or contract, whichever is first.

The retention period is seven years from the record-closed date, which is in accordance with the FDIC's Records and Information Management Policy. Hardcopy files are deleted by shredding and the electronic files are deleted after seven years in accordance with the FDIC's Records Retention and Disposition Schedule.

Hardcopy documents are maintained while the inquiry/complaint is open for reference purposes, and are shredded after the inquiry/complaint is closed (this is generally completed within 60 days, except for Fair Lending cases, which may take up to 120 days).