FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

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

for

Office of the Ombudsman (OO) Use of

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

Date Approved by Chief Privacy Officer (CPO)/Designee: 12/19/2017

SECTION I – OUTSOURCED INFORMATION SERVICE DESCRIPTION

1. Describe the outsourced service and its purpose.

The Enterprise Public Inquiry and Complaints (EPIC) effort will be an enterprise Software as a Service (SaaS) solution that is built on the Salesforce platform. It will be a configured solution to manage public and banker complaints and inquiries received by the Federal Deposit Insurance Corporation (FDIC). The methods of communication to be managed within EPIC include complaints and inquiries received via telephone, email, web-forms, mail, and fax. EPIC is available to Office of the Ombudsman (OO) staff in Washington (Headquarters) and in the Atlanta, Chicago, Dallas, Kansas City, New York, and San Francisco Regional Offices. OO users of EPIC cannot produce reports on individuals using PII because the OO EPIC business administrators scrub the system for PII no less than weekly. All PII noted during the scrub is removed from the system. OO's use of EPIC does not request information on who submitted the complaint/inquiry. OO users will not track responses.

The solution will be acquired and delivered in phases. The initial 2017 scope of work involves 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 (replacing CTS-OATS); and

-Division of Consumer Protection's (DCP's) Specialized Tracking and Reporting System (replacing STARS)

DOA's Customer Communication and Tracking System (CCATS) will be replaced in 2018.

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.

Office of the Ombudsman (OO) in EPIC

OO, through EPIC, tracks inquiries and complaints against the FDIC from the financial industry and the public. OO functions in EPIC will not store personally identifiable information (PII).

The majority of the OO EPIC data entered into the application is done via manual data input from phone calls; no PII is collected via this method. The second method of data collection is via an online FDIC Comment Form located on FDIC.Gov. The only element of PII that is officially collected or asked for on the FDIC.gov form is the complainant's email address (though this is optional); however, there is a comment field that allows free input. Any PII entered into the FDIC Comment Form text fields will be removed by the OO EPIC business administrators and will not be retained in the application or database. The complainant's email address, if voluntarily provided, is retained in EPIC. The OO staff reviews the comment fields no less than weekly to eliminate any PII. The

comments are imported into EPIC, where the OO staff adds all other required data such as the proper issue group, keyword (if any), FDIC division, additional comments, and case resolution.

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 complaints.

Supervisory records are kept logically separated in the EPIC solution.

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

EPIC is used by OO to track inquiries and complaints against the FDIC from the financial industry and the public.

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 OO is the full name of the OO user, and the email address of the complainant when voluntarily provided. Any of the following may be collected through the open text field of the online comment form, but will be removed by OO staff.

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

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: N/A

b) Provide the legal authority which permits the collection of SSNs. N/A

c) Identify whether the SSN is masked or otherwise truncated as part of the outsourced service: N/A

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?**
Members of the Public (via FDIC Comment Form on FDIC.gov)	Inquiry and Complaints Data and the email address of the complainant (when volunteered). Any other PII may be included in the free text field on the online comment form, but is deleted by OO staff when discovered during the weekly scrub..	☒ Yes ☐ No
FDIC Personnel	OO personnel will manually enter OO complaint data such as subject of complaint, division or office complained about, nature of the complaint code (this will not include PII data); DIT personnel will enter OO users' full name in the EPIC system for account creation and management.	☒ Yes ☐ No
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 complainant 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

[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.

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)?

No, data cannot be retrived using a personal identifier. Data is retrieved based on comment/complaint types.

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

N/A

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 thru 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 -OO personnel will have access to the potential PII supplied by complainants in the course of their work, and while doing the weekly scrub to remove PII. OO users will also see the names of their co-workers within EPIC to see who is managing cases, to manage caseloads through the EPIC system, and to communicate within in the EPIC system. -FDIC/DIT Salesforce System admins have access to the potential PII supplied by complainants and the names of OO users assigned to cases in EPIC in order to enable new users or remove users. SYSTEMS OO's use of EPIC shares email addresses with Microsoft Outlook 365 in order for OO users to communicate with the complainant via email (when complainant provides their email address). FDIC CONTRACTORS FDIC Salesforce Integrator support contractors will have access to the potential PII supplied by complainants and the names of OO users assigned to cases in EPIC to build and support the system to FDIC specifications.
10c. Individual Members of the Public (e.g., bidders, investors, borrowers, customers, etc.)	☐	☒	N/A – no members of the public wil have access to any PII contained within EPIC.
10d. Other Non-FDIC Entities/ Parties and/or Non-FDIC Systems/Applications	☐	☒	N/A
10e. Federal, State,	☐	☒	N/A

and/or Local Agencies			
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)	☒	☐
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.

Individuals may provide PII in the open text comment field, sometimes inadvertently, in the online form. When this occurs, EPIC OO administrators remove PII from the free text fields. Individuals have to opt in to providing their e-mail address in the online web form, it is not required.

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 contract with Salesforce.

☒ 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, (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 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.