PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:				
Division/Office:			**Branch or Section:**	
JCAM Name (if applicable):			**JCAM ID (if applicable):**	
Type of Project or Program:	Choose an item.	If “Other,” please describe: Click here to enter text.	**Operational Status:**	Choose an item.
Date PTA Submitted:	Click or tap to enter a date.		**Date of Last PTA:**	Click or tap to enter a date.
Launch Date:	Click or tap to enter a date.			
Authorization Date:	Click or tap to enter a date.		**Authorization Boundary:**	
Reason for PTA:	Choose an item.			

PROJECT MANAGER

Name:			
Division:		**Title:**	
Email:			

PROGRAM MANAGER OR SYSTEM OWNER

Name:			
Division:		**Title:**	
Email:			

INFORMATION SYSTEMS SECURITY MANAGER (ISSM) OR INFORMATION SECURITY MANAGER (ISM)

Name:	
Email:	
Division/Office:	

1. Description Please provide a general description of the project, program, or system and its purpose in a way a non-technical person could understand. If this is an updated PTA, please describe what changes and/or upgrades are triggering the update to this PTA. If this is a renewal, please state whether or not there were any changes to the project, program, or system since the last version. If this update is tied to an SIA, please provide information related to the SIA.
1(a). Authority 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).

1(b). Does the system use PII for research, testing, or training? Select all applicable.	☐ Research ☐ Testing ☐ Training ☐ AI Training ☐ Not applicable

2. Does this system/project/program employ any of the following technologies? (check all that apply)	☐ Cloud Computing ☐ Data Aggregation/Analytics ☐ Social Media

	☐ Web-based application (e.g., SharePoint) ☐ Artificial Intelligence/Machine Learning (AI/ML) • If yes, answer 2(a) and 2(b) ☐ Persistent Tracking Technology ☐ Mobile Applications ☐ None of these
2(a). Select a category that best describes the use of AI	Choose an item.
2(b). Does the purpose of the AI/ML fit within one or more of the use case categories listed? If so, check all that apply.	☐ Scheduling internal-to-government meetings or appointments or setting reminders using AI ☐ Logging and analyzing time spent on tasks using AI-powered time management tools. ☐ Transcribing, summarizing, or other efforts that improve the accessibility of a virtual meeting or interview using AI ☐ Prioritizing and categorizing incoming emails using AI ☐ Editing images, videos, or other public affairs materials using AI ☐ Scheduling and managing social media posts using AI ☐ Generating first drafts of documents, briefing, or communication materials using AI ☐ Improving the quality of written communications using AI tools ☐ Summarizing the key points of a lengthy report using AI ☐ Creating visual representations of data sets for reports or presentations using AI ☐ Using AI-assisted tools in word processors ☐ Generating code using AI ☐. Searching for agency information using a knowledge retrieval system ☐ Identifying and cataloging items in a storage room using AI-driven image recognition ☐ Managing or implementing security controls for information systems (e.g., cybersecurity) using AI ☐ Managing and prioritizing internal service or help desk tickets using AI ☐ Curating news articles and updates based on user preferences using AI ☐ Planning travel routes using AI-driven map applications ☐ Finding and booking travel accommodations using AI-powered platforms

	☐ Unlocking smartphones or other devices without the need for passwords or PINs using AI-based facial recognition technology ☐None of the Above If "none of the above" describe below in 2(c)
2(c). Describe any other purpose(s) of the AI (purposes not listed in 2(a)).	

3. Who provides the information the system/project/program collects, maintains, uses, or disseminates? *Please check all that apply.*	☐ Members of the public ☐ Financial institutions ☐ Loan servicers ☐ Employees of other federal, state, local, and/or territorial governments ☐ FDIC employees/contractors ☐ Internal FDIC systems and records ☐ Third Party Affiliates ☐ Foreign Governments ☐ Non-US Companies or Individuals ☐ Other If "Other" is selected, please describe: **Click here to enter text.**
4. Who are the individuals whose data is collected, maintained, used, or disseminated by the system/project/program? *Please check all that apply. Note that a direct collection means getting the data from the individual (e.g., submission of a form, data entry) and an indirect collection means the data has been acquired through other means (e.g., from another system).*	

Category of Individual	Direct	Indirect
Members of the public	☐	☐
Please describe: Click here to enter text.		
FDIC employees	☐	☐
Contractors	☐	☐
Employees of other federal agencies	☐	☐

4(a). Does the system maintain audit log information? If so, about whom? *Please check all that apply.*	☐ This system does not maintain audit log information ☐ Members of the public ☐ FDIC employees/contractors ☐ Employees of other federal agencies ☐ Other Audit Log Types ☐ Not Applicable, this is not a system
4(b). What PII elements are contained in the audit log?	☐ The audit log does not contain PII ☐ The system elements cited in Question 5 ☐ Other: (Specify) ☐ Not Applicable

5. What PII is created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of? Please mark appropriately below. *Make sure you include unstructured data, if applicable.*

PII Element	Yes	Included in Audit Log?	Are Records Retrieved by PII Element?
1. Full Name	☐	☐	☐
2. Date of Birth	☐	☐	☐
3. Place of Birth	☐	☐	☐
4. Social Security number (SSN)	☐	☐	☐
5. Employment Status, History or Information	☐	☐	☐
6. Mother's Maiden Name	☐	☐	☐

7. Certificates (e.g., birth, death, naturalization, marriage)	☐	☐	☐
8. Medical Information (e.g., Medical Records Numbers, Medical Notes, or X-rays)	☐	☐	☐
9. Home Address	☐	☐	☐
10. Phone Number(s)	☐	☐	☐
11. Email Address	☐	☐	☐
12. Employee Identification Number (EIN)	☐	☐	☐
13. Financial Information (e.g., checking account #, PINs, passwords, credit report, financial transactions)	☐	☐	☐
14. Driver's License/State Identification Number	☐	☐	☐
15. Vehicle Identifiers (e.g., license plates)	☐	☐	☐
16. Legal Documents, Records, or Notes (e.g., divorce decree)	☐	☐	☐
17. Education Records	☐	☐	☐
18. Criminal History Information	☐	☐	☐
19. Military Status and/or Records	☐	☐	☐
20. Investigative Reports and/or Records	☐	☐	☐
21. Biometric Identifiers (e.g., fingerprint, voiceprint)	☐	☐	☐
22. Location Data (e.g., travel information, mobile phone location, etc.)	☐	☐	☐
23. Photographic Identifiers (e.g., image, x-ray, video)	☐	☐	☐
24. NTID/UUID	☐	☐	☐
25. Eligibility Data (e.g., information concerning an individual's eligibility for a government benefit,	☐	☐	☐

job, clearance, contract, or payment from the FDIC)			
26. Other (Specify: ____)	☐	☐	☐

5(a). If SSN is checked above, please provide the specific legal basis, purpose for the collection of the SSN, and intended uses of the SSN.	
5(b). Does the project, program, or system retain an accounting of disclosures?	☐ Yes ☐ No ☐ The system or project does not maintain an accounting of disclosures. The disclosures are being made to individuals with a need to know. Therefore, the system or project is not required to keep an accounting of disclosures. ☐ The system or project does not maintain an accounting of disclosures. The disclosures are being made a to a law enforcement agency pursuant to a 5 U.S.C. § 552a (b)(7) request. Therefore, the system or project is not required to keep an accounting of disclosures. ☐ The system or project is not a system of records under the Privacy Act, and FDIC is therefore not required to maintain an accounting of disclosures. ☐ The system or project does not maintain an accounting of disclosures. FDIC Chairman has promulgated rules that exempt this system or project from the requirement to provide the accounting of disclosures to individuals under the Privacy Act of 1974, as amended. Therefore, the system or project is not required to keep an accounting of disclosures.
5(c): Does this information system or project make a computerized comparison of two or more automated systems of records, or a system of records with non-federal records, for the purpose	☐ Yes. If yes, please list the Computer Matching Agreement: ☐ No

of establishing or verifying eligibility or compliance as it relates to cash or in-kind assistance or payments under federal benefit programs?	
5(d): Does the collection or processing of information described above actually or potentially impact an individual who is exercising rights guaranteed by the First Amendment (e.g., free speech, religion, right to assemble, etc.). If yes, please explain. Note: the processing of information describing how any individual exercises rights guaranteed by the First Amendment is prohibited unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity .	☐ Yes. If yes, explain: ☐ No
5(e): Describe de-identification methods used to manage privacy risks, if applicable.	

6. Describe if this project, program, or system connects, receives, or shares PII with any other FDIC programs or systems.

Source	List the PII elements that are received (See Question 5)

Destination	List the PII elements that are shared (See Question 5)

7. Describe if this project, program, or system connects, receives, or shares PII with any other external (non-FDIC) programs, systems, or the public.

Source	List the PII elements that are received (See Question 5)

Destination	List the PII elements that are shared (See Question 5)

7(a). Is this external sharing pursuant to new or existing information access sharing agreement (MOU, MOA, LOI, Contract, LSA, etc.)?	Choose an item. **Please describe the applicable information sharing governance in place, and provide a copy of the information sharing agreement to Privacy for review:**

7(b). Have you completed Form 3700-60, indicating that the privacy Contract Clauses in any external contractual agreement have been reviewed by FDIC Privacy as applicable?	☐ N/A ☐ Yes ☐ No If "No" is selected, please describe:
7(c). Please provide the solicitation or contract number(s).	☐ N/A ☐ Contract number: #### ☐ Solicitation number: ####

8. Please provide an estimate of the number of individuals whose PII is contained within the project/program/system.	
8(a). Explain how the number was derived.	
9. Will the system/project/program use any forms (paper or electronic) to collect data?	☐ Yes **If yes, please select all applicable:** ☐ Paper ☐ Electronic ☐ No
9(a). What is the form number, if applicable?	
10. Has Records and Information Management Unit (RIMU) established a Records Schedule for this data collection?	

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY THE OCISO PRIVACY SECTION)

OCISO Privacy Section Reviewer:	
Date approved by OCISO Privacy Section:	Click or tap to enter a date.

DESIGNATION

Does the System, Project, or Program collect, maintain, include, process, or otherwise involve PII?	**Choose an item.**
Category of System, Project, or Program:	**Choose an item.** If "other" is selected, please describe: Click here to enter text.
Is a Negligible Risk Worksheet (NRW) being completed for this system, project, or program?	**Choose an item.**
What is the FIPS 199 determination?	Confidentiality: ☐ Low ☐ Moderate ☐ High Integrity: ☐ Low ☐ Moderate ☐ High Availability:

	☐ Low ☐ Moderate ☐ High
What is the Privacy Categorization Recommendation?	Confidentiality: ☐ Low ☐ Moderate ☐ High Integrity: ☐ Low ☐ Moderate ☐ High Availability: ☐ Low ☐ Moderate ☐ High

Determination:	☐ PTA sufficient at this time. ☐ Privacy Act Statement required; Published: [describe location: e.g., form] ☐ Privacy Notice required; Published: [describe location: e.g., form] ☐ Privacy Impact Assessment (PIA) required. ☐ System of Records Notice (SORN) required. ☐ Privacy Controls required. Controls specified below.
PIA:	**Choose an item.** If covered by existing PIA, please list:
SORN:	**Choose an item.** If covered by existing SORN, please list: ☐ Exemptions apply.
Privacy Controls:	**Choose an item.** ☐ AI Controls Overlay

	Additional Applicable Controls:
Is this PTA a component of an authorized system or subsystem? NIST defines component as: "A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware."	**Choose an item.**

OCISO Privacy Program Comments: *Please describe rationale for privacy compliance determination above.*
[PII – X, PIA – X [List PIAs], SORN – X [List SORNs], Privacy Controls – Privacy Baseline/None, AI - X, SSN – X]

NIST 800-53 Rev. 5 Tailored Implementation Statements	
AC-03(14): Access Enforcement | Individual Access *(NIST Privacy Baseline)*	If the data covered by this PTA requires a Privacy Act system of records notice, insert: "PROVIDE [PRIVACY ACT ACCESS PROCEDURES PROMULGATED VIA REGULATIONS AVAILABLE AT 12 C.F.R. § 310] TO ENABLE INDIVIDUALS TO HAVE ACCESS TO THE FOLLOWING ELEMENTS OF THEIR PERSONALLY IDENTIFIABLE INFORMATION: PII MAINTAINED IN FDIC SYSTEM(S) OF RECORDS IN ACCORDANCE WITH THE PRIVACY ACT]." If the system permits specialized individual access to data elements in the system, develop custom implementation statement describing the procedures and which PII elements are accessible. Or, "NOT REQUIRED."
AC-16(05): Security and Privacy Attributes | Attribute Displays on Objects to Be Output *(AI Overlay)*	[Insert system name] WILL HAVE TO DISPLAY SECURITY AND PRIVACY ATTRIBUTES IN HUMAN-READABLE FORM ON EACH OBJECT THAT THE SYSTEM TRANSMITS TO OUTPUT DEVICES TO IDENTIFY DATA WITH AN ATTRIBUTE VALUE OF "TRUE" FOR "ISAIGENERATED" ATTRIBUTE USING LABELS, TAGS, OR OTHER INDICATORS THAT IDENTIFY THE DATA AS "AI GENERATED" TO THE USER.
AU-03(03): Content of Audit Records | Limit Personally Identifiable Information Elements *(NIST Privacy Baseline)*	If there are audit logs, insert "FDIC LIMITS THE PERSONALLY IDENTIFIABLE INFORMATION CONTAINED IN AUDIT RECORDS IN [SYSTEM NAME] TO THE FOLLOWING ELEMENTS IDENTIFIED IN THE PRIVACY RISK ASSESSMENT: [PII IN THE AUDIT LOGS AS LISTED IN THE PTA SPECIFIC TO THE SYSTEM OR PROJECT OR THE [SYSTEM NAME] PTA VALIDATES THE NEED FOR PII IN AUDIT RECORDS."] If no audit logs, insert "[SYSTEM NAME] DOES NOT GENERATE AUDIT LOGS."
PL-02: System Security and Privacy Plans *(NIST Privacy Baseline)*	"FDIC COMPLETES PRIVACY PLANS THROUGH THE CONDUCT OF A PRIVACY THRESHOLD ANALYSIS, WHICH DETERMINES WHAT ADDITIONAL PRIVACY REQUIREMENTS APPLY." If FDIC is doing a control assessment, insert "THE REQUIREMENTS INCLUDE IDENTIFYING THE NECESSARY CONTROLS TO BE IMPLEMENTED, ASSESSED, AND CONTINUOUSLY MONITORED. THE PRIVACY PLAN FOR [SYSTEM NAME] IS PRODUCED AS A REPORT FROM JCAM."
PL-04: Rules Of Behavior *(AI Overlay)*	For systems using AI, establish supplemental rules of behavior that incorporate AI specificities to include at a minimum, the requirements to: 1. Have completed any required initial and reoccurring AI security/privacy training. 2. Conduct reviews of AI-generated content for accuracy, appropriateness, and actual usefulness before being accepted. 3. Record and report instances of malicious, vulnerable, erroneous, or false AI-generated content; AI behavior or output that is inconsistent with expectations; and/or unauthorized disclosure of PII or other FDIC information to applicable parties such as SRT, the System owner, and vendor.

PL-04(01) Rules Of Behavior | Social Media And External Site/Application Usage Restrictions
(NIST Privacy Baseline)
	A. THE RULES OF BEHAVIOR INCLUDE RESTRICTIONS ON THE USE OF SOCIAL MEDIA, SOCIAL NETWORKING SITES, AND EXTERNAL SITES/APPLICATIONS;
	B. THE RULES OF BEHAVIOR INCLUDE RESTRICTIONS ON POSTING ORGANIZATIONAL INFORMATION ON PUBLIC WEBSITES;
	C. THE RULES OF BEHAVIOR INCLUDE RESTRICTIONS ON THE USE OF ORGANIZATION-PROVIDED IDENTIFIERS (E.G., EMAIL ADDRESSES) AND AUTHENTICATION SECRETS (E.G., PASSWORDS) FOR CREATING ACCOUNTS ON EXTERNAL SITES/APPLICATIONS.

PM-21: Accounting of Disclosures *(NIST Privacy Baseline)*	Common Control Provider: Privacy Program, OCISO The Senior Agency Official for Privacy (SAOP) periodically consults with managers of organization systems of record to ensure that the required accountings of disclosures of records are being properly maintained and include: 1. Date, nature, and purpose of each disclosure; and 2. Name and address, or other contact information of the individual or organization to which the disclosure was made b. FDIC retains the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and c. Makes the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request. System Level Responsibility: SYSTEM OWNERS ARE RESPONSIBLE FOR CREATING AN ACCOUNTING OF DISCLOSURES WHEN ASKED. Note: Check the PTA and/or PIA for a determination of whether a SORN is required. If there is a SORN, insert the following language: “THE FDIC RETAINS THE ACCOUNTING OF DISCLOSURES AS SPECIFIED BY THE PRIVACY ACT OF 1974 AND FDIC DIRECTIVE 1360.20 PRIVACY PROGRAM.” If there is no SORN, insert the appropriate language: 1. THE SYSTEM OR PROJECT DOES NOT MAINTAIN AN ACCOUNTING OF DISCLOSURES. THE DISCLOSURES ARE BEING MADE TO INDIVIDUALS WITH A NEED TO KNOW. THEREFORE, THE SYSTEM OR PROJECT IS NOT REQUIRED TO KEEP AN ACCOUNTING OF DISCLOSURES. 2. THE SYSTEM OR PROJECT DOES NOT MAINTAIN AN ACCOUNTING OF DISCLOSURES. THE DISCLOSURES ARE BEING MADE A TO A LAW ENFORCEMENT AGENCY PURSUANT TO A 5 U.S.C. § 552A(B)(7) REQUEST. THEREFORE, THE SYSTEM OR PROJECT IS NOT REQUIRED TO KEEP AN ACCOUNTING OF DISCLOSURES. 3. THE SYSTEM OR PROJECT IS NOT A SYSTEM OF RECORDS UNDER THE PRIVACY ACT, AND FDIC IS THEREFORE NOT REQUIRED TO MAINTAIN AN ACCOUNTING OF DISCLOSURES. 4. THE SYSTEM OR PROJECT DOES NOT MAINTAIN AN ACCOUNTING OF DISCLOSURES. FDIC CHAIRMAN HAS PROMULGATED RULES THAT EXEMPT THIS SYSTEM OR PROJECT FROM THE REQUIREMENT TO PROVIDE THE ACCOUNTING OF DISCLOSURES TO INDIVIDUALS UNDER THE PRIVACY ACT OF 1974, AS AMENDED. THEREFORE, THE SYSTEM OR PROJECT IS NOT REQUIRED TO KEEP AN ACCOUNTING OF DISCLOSURES.

PT-03: Personally Identifiable Information Processing Purposes *(NIST Privacy Baseline)*	Common Control Provider: Privacy Program, OCISO c. FDIC Implements organization level controls to ensure PII is processed only for stated purposes using a variety of technologies such as DLP, device configurations to restrict the use of external storage devices, web content reviews and approvals and any additional control requirements as required by Privacy as documented in the PTA; and d. Privacy Program monitors changes in the processing of personally identifiable information through the SIA submission and approval process. System Owners are required to submit an SIA any time there is a change in PII processing. Privacy Program has implemented policies and procedures to ensure that any changes are made in accordance with applicable federal and FDIC requirements in accordance with FDIC Directive 1360.20 Privacy Program. System Level Responsibility: System Owners are responsible for: a. Ensuring the purpose(s) for processing PII are identified and documented in the appropriate Privacy documents and publicly facing notices; b. Describing the purpose(s) in the following public privacy notices and policies of the organization; c. Implementing system level controls to ensure PII is processed only for stated purposes; and d. Submitting an SIA any time there is a change in PII processing [INSERT PURPOSE LANGUAGE AS WRITTEN IN QUESTION 1 DESCRIPTION FROM THE PTA] [IF A SOR: “THE PURPOSE OF THIS SYSTEM IS CONSISTENT WITH THE PURPOSE STATED IN THE APPLICABLE SORN(S)]
PT-04: Consent *(NIST Privacy Baseline)*	“FOR [INSERT SYSTEM NAME], FDIC HAS PROVIDED [IF A PRIVACY ACT STATEMENT, "A PRIVACY ACT STATEMENT"; IF A PRIVACY NOTICE, “A PRIVACY NOTICE"] FOR INDIVIDUALS TO CONSENT TO THE PROCESSING OF THEIR PERSONALLY IDENTIFIABLE INFORMATION PRIOR TO ITS COLLECTION THAT FACILITATE INDIVIDUALS’ INFORMED DECISION-MAKING.” Or "NOT REQUIRED."

PT-05: Privacy Notice *(NIST Privacy Baseline)*	***NOTE: If contractor system, control is Contractor responsibility*** Common Control Provider: Privacy Program, OCISO Privacy Program creates Privacy notices that b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language; c. Identifies the authority that authorizes the processing of personally identifiable information; d. Identifies the purposes for which personally identifiable information is to be processed; and e. Includes any additional information required by the PTA OCISO Privacy Program. System Level Responsibility: a. System Owners are responsible for providing notices to individuals about the processing of PII upon interacting with the system and subsequently at any point of the collection. [IF NOTICE IS GIVEN, IDENTIFY WHERE: FORM, SPLASH PAGE, READ, OTHER, ETC.] Or "NOT REQUIRED."
PT-05(02): Privacy Notice | Privacy Act Statements *(NIST Privacy Baseline)*	"For [INSERT SYSTEM NAME], FDIC provides a Privacy Act statement on [INSERT FORM NAME] or provides Privacy Act statements [EXPLAIN WHERE THE PRIVACY ACT STATEMENT IS LOCATED.]" Or "NOT REQUIRED."

PT-06: System of Records Notice *(NIST Privacy Baseline)*	Common Control Provider: Privacy Program, OCISO OMB Legal a. Privacy Program uses the Privacy Threshold Analysis to determine if a System of Records Notice is required in accordance with the Privacy Act of 1974 and OMB Circular A-108, ‘Federal Agency Responsibilities for Review, Reporting, and Publication.’ If a SORN has been determined to be required, the Privacy Program will coordinate with the System Owners and ISSMs to create the SORN and uploaded into JCAM. b. The FDIC submits SORNs to OMB and Congress at least 30 days prior to publishing them in the Federal Register to allow for review and comments for the agency. Upon being published in the Federal Register, the SORN provides the opportunity for individuals to submit questions or comments about the system and its routine uses for 30 days before any disclosure of information takes place. The 30-day comment period by OMB and the 30-day Federal Register publication cannot run concurrently. System Level Responsibility: c. System Owners are responsible for keeping the system of records notices accurate, up-to-date, and scoped in accordance with policy by: • Reviewing Privacy documents at least annually to determine if there are any significant changes in the collection, processing or storage of PII as defined by OMB circular A-108; • Submitting an SIA for privacy to determine if a change to the PTA, PIA and SORN is required; and • Coordinate with the Privacy Program to update the PTA, PIA and SORN as required. [INSERT THE SORN, IF REQUIRED FROM THE PTA. IF NO SORN REQUIRED, STATE "NOT REQUIRED."]

PT-06(01): System of Records Notice | Routine Uses *(NIST Privacy Baseline)*	Common Control Provider: Privacy Program, OCISO Privacy Program reviews the PTA and SORN to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was collected. SORNs are continuously monitored and modified when a system of records undergoes a significant change. System Level Responsibility: System Owners are responsible for reviewing all routine uses published in the system of records notice to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was collected by: • Reviewing Privacy documents at least annually to determine if there are any significant changes in the collection, processing or storage of PII as defined by OMB circular A-108; • Submitting an SIA for privacy to determine if a change to the PTA, PIA and SORN is required; and • Coordinate with the Privacy Program to update the PTA, PIA and SORN as required. [INSERT THE SORN, IF REQUIRED FROM THE PTA. IF NO SORN, STATE "NOT REQUIRED."]]
PT-06(02): System of Records Notice | Exemption Rules *(NIST Privacy Baseline)*	Common Control Provider: Privacy Program, OCISO Privacy Program reviews all Privacy Act exemptions claimed for the system of records to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are accurately described in the system of records notice. System Level Responsibility: System Owners are responsible for reviewing all Privacy Act exemptions claimed for the system of records to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are accurately described in the system of records notice by: • Reviewing Privacy documents at least annually to determine if there are any significant changes in the collection, processing, or storage of PII as defined by OMB circular A-108; • Submitting an SIA for privacy to determine if a change to the PTA, PIA, and SORN is required; and • Coordinate with the Privacy Program to update the PTA, PIA, and SORN as required. [INSERT THE SORN, IF REQUIRED FROM THE PTA. IF NO SORN, STATE "NOT REQUIRED."]

PT-07: Specific Categories of Personally Identifiable Information *(NIST Privacy Baseline)*	***NOTE: If contractor system, control is Contractor responsibility*** Common Control Provider: Privacy Program, OCISO Privacy Program uses the Privacy Threshold Analysis to establish any approved conditions or protections that may be necessary for specific categories of personally identifiable information. System Level Responsibility: [NONE] [OR [INSERT ANY SPECIFIC CONDITIONS OUTLINED IN THE PTA]
PT-07(01): Specific Categories of Personally Identifiable Information | Social Security Numbers *(NIST Privacy Baseline)*	a. [INSERT SYSTEM NAME] does/does not process Social Security numbers [INSERT: WHEN SSNS ARE INCIDENTAL OR POSSIBLE "ALTHOUGH THE SYSTEM MAY HOST APPLICATIONS OR PROCESSES THAT DO"]. FDIC uses the Privacy Threshold Analysis to identify when SSNs are collected and to validate that the collection, maintenance, and use of Social Security number may not be eliminated further. b. The FDIC does not deny any individual any right, benefit, or privilege provided by law because of such an individual's refusal to disclose his or her SSN. c. [SELECT THE APPROPRIATE OPTION(S): 1. WHEN THE FDIC COLLECTS THE SSN DIRECTLY FROM THE INDIVIDUAL, INSERT "THE FDIC INFORMS THE INDIVIDUAL WHETHER THAT DISCLOSURE IS MANDATORY OR VOLUNTARY, BY WHAT STATUTORY OR OTHER AUTHORITY SUCH NUMBER IS SOLICITED, AND WHAT USES WILL BE MADE OF IT, WHEN THE FDIC COLLECTS THE SSN DIRECTLY FROM THE INDIVIDUAL. [SELECT AS APPROPRIATE: "SEE PT-5-05 PRIVACY NOTICE AND/OR PT-5-05(2): PRIVACY ACT STATEMENT"]. 2. WHEN THE FDIC DOES NOT COLLECT THE SSN DIRECTLY FROM THE INDIVIDUAL, INSERT "THE [INSERT SYSTEM] DOES NOT COLLECT THE SSN DIRECTLY FROM THE INDIVIDUAL AND THEREFORE DOES NOT INFORM HE INDIVIDUAL WHETHER THAT DISCLOSURE IS MANDATORY OR VOLUNTARY, BY WHAT STATUTORY OR OTHER AUTHORITY SUCH NUMBER IS SOLICITED, AND WHAT USES WILL BE MADE OF IT." OR 3. WHEN THE FDIC DOES NOT COLLECT SSNS, INSERT ["INSERT SYSTEM NAME] DOES NOT PROCESS SOCIAL SECURITY NUMBERS, THEREFORE NO NOTIFICATION IS REQUIRED."]

PT-07(02): Specific Categories of Personally Identifiable Information | First Amendment Information *(NIST Privacy Baseline)*	"[SYSTEM NAME] MAY NOT PROCESS INFORMATION DESCRIBING HOW ANY INDIVIDUAL EXERCISES RIGHTS GUARANTEED BY THE FIRST AMENDMENT UNLESS EXPRESSLY AUTHORIZED BY STATUTE OR BY THE INDIVIDUAL OR UNLESS PERTINENT TO AND WITHIN THE SCOPE OF AN AUTHORIZED LAW ENFORCEMENT ACTIVITY." If there is statutory authorization, individual authorization (consent), and/or an authorized law enforcement activity supporting the collection of First Amendment information, insert: "[SYSTEM NAME] IS AUTHORIZED TO COLLECT FIRST AMENDMENT INFORMATION PURSUANT TO [INSERT CITATION TO STATUTE, FORM USED TO COLLECT INDIVIDUAL'S WRITTEN CONSENT, AND/OR DESCRIPTION OF AUTHORIZED LAW ENFORCEMENT ACTIVITIES.]" If the program lacks statutory authority and does not collect an authorization from the individual, insert: "[SYSTEM NAME] DOES NOT HAVE STATUTORY AUTHORITY OR INDIVIDUAL AUTHORIZATION TO COLLECT THIS INFORMATION." If the program is not engaging in authorized law enforcement activities to which the information is pertinent or within the scope of, insert: "THE PROCESSING OF THIS INFORMATION BY [SYSTEM NAME] IS NOT WITHIN THE SCOPE OF OR PERTINENT TO AN AUTHORIZED LAW ENFORCEMENT ACTIVITY."

RA-03: Risk Assessment *(NIST Privacy Baseline)*	***For FDIC owned and managed systems only*** Common Control Providers: Cyber Risk Management Section (CRMS), OCISO Enterprise Security Operations Section (ESOS), OCISO Privacy Program, OCISO a. The CRMS SCA Team conducts a risk assessment on all FDIC internal systems by conducting annual security assessments in accordance with the SCA Methodology. ESOS conducts weekly vulnerability scanning as documented in RA-05 The Privacy Program uses the PTA and PIA as applicable in order to: 1. Identifying threats to and vulnerabilities in the system; 2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and 3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information b. FDIC integrates risk assessment results and risk management decisions into the SCA, vulnerability scanning and privacy processes; c. The CRMS SCA team develops an Executive Summary which provides a high-level overview of the results of the assessment which will include: • Tables and charts for any control failures; • A detailed description of each control failure including: o The associated risk; o A proof-of-concept to recreate the issue; o A misuse case to explain the impact of the issue; and o One or more recommendations to resolve the issue. • An Appendix containing test procedures and results for each control, and the status (e.g., Pass, Fail, or N/A) of the control at time of the SCA. ESOS documents security scan result in various dashboards within Security Center and documents unmitigated risks in the form of POA&Ms in JCAM; The Privacy Program publishes the PTA and PIA as applicable d. The CRMS SCA team reviews the risk assessment annually as part of the annual SCA assessment cycle e. Provides the results of the control assessment to individuals or roles defined in the FDIC Assessment and Authorization Process Guide. ESOS documents security scan result in various dashboards within Security Center. Privacy Program provides the results in the PTA and PIA; and f. The CRMS SCA team updates the risk assessment annually as part of the annual SCA assessment cycle. Nessus automatically updates the dashboards in Security Center on a continuous basis System Level Responsibility: System Owners are responsible for: d. Reviewing risk assessment results in the SCA Report, Vulnerability reports in Security Center and POA&Ms in JCAM; f. Updating POA&M status and milestones at least monthly. [INSERT NAME OF THE PTA, CONDUCTED; AND THE NAME OF THE PIA, AS APPLICABLE FROM THE PTA]

	If FDIC is not conducting a controls assessment use: “Common Control Provider: Cyber Risk Management Section (CRMS), OCISO Enterprise Security Operations Section (ESOS), OCISO Privacy Program, OCISO a. The Privacy Program uses the PTA and PIA as applicable in order to: 1. Identify threats to and vulnerabilities in the system; 2. Determine the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and 3. Determine the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information b. FDIC integrates risk assessment results and risk management decisions into privacy processes; c. The Privacy Program publishes the PTA and PIA as applicable; and e. The Privacy Program provides the results in the PTA and PIA; [INSERT SYSTEM NAME] PTA The implementation of the remainder of this control is the responsibility of the contractor.”

RA-08: Privacy Impact Assessment *(NIST Privacy Baseline)*	Common Control Provider: Privacy Program, OCISO a., & b. The Privacy Program conducts a privacy impact assessment based on the information contained in the system level PTA for systems, programs, or other activities developing or procuring information technology that PII information and when initiating a new collection of PII that will be processed. This include PII permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government. The PIA process is conducted in accordance with FDIC Directive 1360.20 Privacy Program, FDIC PIA User Guide, and PIA Template. System Level Responsibility: System Owners are responsible for ensuring a PTA has been submitted to Privacy to determine of a PIA is required and to submit an SIA any time there is a significant change to the collection, processing, dissemination or storage of PII as defined by OMB A-108 for Privacy to review and determine if the PIA requires updating. [INSERT NAME OF THE PIA, IF REQUIRED, FROM THE PTA. IF NO PIA IS REQUIRED, "NOT REQUIRED." DO NOT INCLUDE DATES OF THE DOCUMENTS.]
SA-04(11) Acquisition Process | System of Records *(FDIC Privacy Enhancement)*	Privacy Act requirement for contracts is as follows: 5 USC 552a(m) (m)(1) GOVERNMENT CONTRACTORS.—When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency If the data covered by this PTA requires a Privacy Act system of records notice, insert “SYSTEM OWNERS ARE RESPONSIBLE FOR ENSURING CLAUSE 7.5.1-01, PRIVACY ACT, IS INCLUDED IN THE ACQUISITION CONTRACT FOR THE OPERATION OF A SYSTEM OF RECORDS ON BEHALF OF THE FDIC TO ACCOMPLISH AN ORGANIZATIONAL MISSION OR FUNCTION.” If there is not a system of records, insert “NOT REQUIRED.”

SA-08(33): Security and Privacy Engineering Principles | Minimization *(NIST Privacy Baseline)*	Common Control Provider: Privacy Program, OCISO FDIC implements the privacy principle of minimization by validating the need for each element when documenting the personally identifiable information processed in accordance with FDIC Directive 1360.20 Privacy Program. System Level Responsibility: System Owners are responsible for documenting how they implement principle of minimization within the Privacy documents. "THE NECESSARY PII ELEMENTS ARE DOCUMENTED IN THE PTA."
SI-10(05): Information Input Validation | Restrict Inputs to Trusted Sources and Approved Formats *(AI Overlay)*	Restrict the use of information inputs to [defined trusted sources] and/or [formats defined by the system owner]. THOSE DEFINED TRUSTED SOURCES ARE LIMITED TO THE FOLLOWING: [List trusted data sources approved for use in the PTA]. Or "NOT APPLICABLE"

SI-12: Information Management and Retention *(NIST Privacy Baseline)*	Common Control Provider DOA, RIMU FDIC manages and retains information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements. System Level “THE DATA IN [INSERT SYSTEM NAME] IS RETAINED IN ACCORDANCE WITH [INSERT "RETENTION SCHEDULE" OR "BUSINESS NEED PENDING APPROVAL OF A RETENTION SCHEDULE"] AND THEREAFTER DESTROYED IN ACCORDANCE WITH MP-6 AND SI-12(3).” For platforms, insert the following: "THE DATA IN [THE SYSTEM] IS RETAINED IN ACCORDANCE WITH THE RETENTION SCHEDULES ESTABLISHED AT THE APPLICATION LEVEL, AND THEREAFTER DESTROYED IN ACCORDANCE WITH MP-6-06 AND SI-12(3)."

SI-12(01): Information Management and Retention | Limit Personally Identifiable Information Elements *(NIST Privacy Baseline)*	FDIC limits personally identifiable information being processed in [SYSTEM NAME] the information life cycle to the following elements of personally identifiable information: [INSERT THE PII IDENTIFIED IN THE PTA SPECIFIC TO THE SYSTEM OR PROJECT. IF ALL ELEMENTS, INSERT "ALL PII ELEMENTS IDENTIFIED IN THE PTA", IF ADDITIONAL ELEMENTS, LISTED UNDER "OTHER," LIST THOSE PII ELEMENTS. IF A SUBSET OF THE LIST IN THE PTA, LIST THE SUBSET OF DATA ELEMENTS.] Full Name Date of Birth Place of Birth Social Security number (SSN) Employment Status, History or Information Mother's Maiden Name Certificates (e.g., birth, death, naturalization, marriage) Medical Information (e.g., Medical Records Numbers, Medical Notes, or X-rays) Home Address Phone Number(s) Email Address Employee Identification Number (EIN) Financial Information (e.g., checking account #, PINs, passwords, credit report, financial transactions) Driver's License/State Identification Number Vehicle Identifiers (e.g., license plates) Legal Documents, Records, or Notes (e.g., divorce decree) Education Records Criminal History Information Military Status and/or Records Investigative Reports and/or Records Biometric Identifiers (e.g., fingerprint, voiceprint) Location Data (e.g., travel information, mobile phone location, etc.) Photographic Identifiers (e.g., image, x-ray, video) NTID/UUID Eligibility Data (e.g., information concerning an individual's eligibility for a government benefit, job, clearance, contract, or payment from the FDIC) Other (Specify: ___________________________________)

SI-12(02): Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training and Research *(NIST Privacy Baseline)*	Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: [FOR RESEARCH AND TRAINING, USE THE METHODS APPROVED BY THE PRIVACY PROGRAM; FOR TESTING, METHODS MUST COMPLY WITH THE FDIC TEST DATA POLICY AND CIOO IT GOVERNANCE AND TEST DATA MANAGEMENT POLICY]. “The adjudication of the PTA serves as authorization to use the PII for research and training purposes on authorized systems by authorized users and use of PII for testing in accordance with the FDIC White Paper ‘Production Data in Lower Environments’ (https://fdicnet.fdic.gov/content/dam/ociso/documents/Whitepaper%20-%20Prod%20Data%20for%20Testing%20-%20August%202020.pdf), FDIC Directive 1360.20 ‘Privacy Program’, and the Fair Information Practice Principles. [ADD CONDITIONS IDENTIFIED IN THE SYSTEM PTA, IF APPLICABLE. EXAMPLES INCLUDE, REDACTION OR MASKING OF DIRECT IDENTIFIERS, BINNING, ETC.]”
SI-18(03) Personally Identifiable Information Quality Operations | Collection *(FDIC Privacy Enhancement)*	“PERSONALLY IDENTIFIABLE INFORMATION IS COLLECTED DIRECTLY FROM THE INDIVIDUAL.” [ADD IMPLEMENTATION LANGUAGE TO DESCRIBE HOW IT WILL SPECIFICALLY WORK FOR THE SYSTEM OR “NOT APPLICABLE” AND EXPLAIN]
SI-19 De-Identification *(NIST Privacy Baseline)*	“SYSTEM OWNER IS RESPONSIBLE FOR: “a. REMOVING THE FOLLOWING ELEMENTS OF PERSONALLY IDENTIFIABLE INFORMATION FROM DATASETS: [INSERT ANY ELEMENTS REMOVED VIA THE PTA AND/OR PIA PROCESS]; and b. EVALUATING THE RESULTS FOR EFFECTIVENESS OF DE-IDENTIFICATION RELATIVE TO THE BUSINESS NEED.” OR ”NOT REQUIRED”