Privacy Impact Assessment (PIA) for FDIC Acquisition Management System (FAMS)

November 8, 2021
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 website, which describes FDIC’s activities that impact privacy, the authority for collecting PII, and the procedures to access and have PII amended or corrected if necessary.

SYSTEM OVERVIEW

The FDIC’s Division of Administration (DOA) Acquisition Services Branch (ASB) is responsible for awarding and administering contracts and purchase orders to support FDIC’s mission, goals and objectives. ASB provides vital procurement and business advisory services to FDIC Divisions and Offices, ensuring that fundamentally sound business practices are integrated within FDIC’s acquisition of goods and services. In support of that responsibility, FDIC is implementing the FDIC Acquisition Management System (FAMS), which leverages a FedRAMP authorized cloud-based software as a service (SaaS) application that will be used by all Divisions and Offices across the Corporation. FAMS provides full procurement life-cycle support for the following FDIC procurement phases:

- **Early Acquisition Planning Phase** – In this phase FDIC program offices develop requirements packages, including drafting statements of work (SOW), conduct market research and collaborate with ASB and other stakeholders prior to submitting requirements packages to DOA ASB.
- **Contract Pre-Solicitation Phase** – In this phase SOWs, acquisition plans, and other required documents are refined.
- **Solicitation Phase** – In this phase detailed solicitation documents are prepared and released to facilitate the submission of responsive proposals from qualified offerors. Proposals subsequently received from offerors are evaluated on the basis of price, past performance, contractor capacity, quality and technical capability, as deemed appropriate for the respective contracts. The successful offeror is determined at the end of this phase.
- **Contract Award Phase** – In this phase the final award decision document is prepared and provided to the successful offeror, while unsuccessful offeror(s) are notified of the award decision.
- **Contract Administration and Document Management Phase** - This phase includes various contract administration activities, such as receiving deliverables, making contract modifications, appointing/removing oversight managers, and evaluating contractor performance.
- **Contract Closeout Phase** - This phase includes verifying that all invoiced work was performed during the contract period of performance, verifying that payments made to the contractor are appropriate, and documenting the closed-out status of the contract.

FAMS also serves as the official contract file for FDIC and will also be used to prepare management reports containing procurement and contract data.

Additionally, in future releases, FAMS will be integrated with Unison’s FedConnect online service. Once the integration between FAMS and FedConnect is fully implemented, FAMS will be used by FDIC FAMS users to seamlessly post solicitations to FedConnect, where they will be available for viewing by the general public. Vendors who wish to contract with FDIC will typically be required to register with FedConnect. Once registered, the vendors will be able to use FedConnect to securely send responses to FDIC solicitations via the FedConnect/FAMS integrated service. The FAMS/FedConnect integrated service will also include a secure messaging service that will allow FDIC FAMS users and vendors to exchange messages via the FAMS/FedConnect integrated service.

---

1 https://www.fdic.gov/policies/privacy/index.html
PRIVACY RISK SUMMARY

In conducting this PIA of FAMS, we 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 and Individual Participation
- Access and Amendment
- Data Minimization
- Data Quality and Integrity
- Purpose and Use Limitation

Transparency and Individual Participation Risk:

Privacy Risk: There is a risk that individuals may not be aware and/or have provided explicit consent for the collection and use of their information within FAMS.

Mitigation: In instances where FAMS is provided PII from non-FDIC systems or entities, including those detailed in Section 1.0 of this PIA, it is incumbent upon the source system or entity to provide any applicable, required notices to the individuals from whom they collected the information. Additionally, this PIA and the SORNs listed in Section 2.2 of this PIA serve as notice of the Federal Government and FDIC's uses of this PII.

Access and Amendment Risk:

Privacy Risk: In some cases, FAMS is provided vendor information, including PII, from a third-party source, as described in Section 1.0 of this PIA. The FDIC has limited ability to implement procedures to correct inaccurate or erroneous information in such cases.

Mitigation: Vendors do not provide PII directly to FAMS. Instead, FAMS receives vendor information, which may include PII, via system interface or via manual entry by FDIC personnel as described in Section 1.0 of this PIA. In such cases, the responsibility to notify individuals falls to the systems/entities that initially collected the information. Additionally, FDIC FAMS users may contact vendors to facilitate the correction and validation of their information. Further, the procedures for amending PII are published in the SORNs listed in Section 2.2 of this PIA.

Data Minimization Risk:

Privacy Risk: There is a risk that the personally identifiable information maintained by FAMS may be unnecessary or excessive, or may be kept longer than is necessary to meet the business need for which it was collected.

Mitigation: This risk is mitigated by FDIC policy regarding the collection, use, and retention of FAMS records, as well as FAMS users being appropriately trained. FAMS follows an approved record retention schedule for the collection, retention and disposal of FAMS records, which may contain PII. FAMS users will be provided training when they are initially provided access to FAMS. Additionally, FAMS refresher courses will be provided on a periodic basis. The FAMS training courses/sessions will include information that addresses the collection, maintenance and protection of PII in conjunction with the procurement and contracting function.

Data Quality and Integrity:

Privacy Risk: There is a potential risk associated with data quality and integrity because vendor information may be manually entered into FAMS by FAMS users.
Mitigation: This risk is mitigated by FAMS users being appropriately trained and by FAMS users reviewing PII contained within records prior to the records being uploaded to FAMS to ensure that the information is correct and current.

Purpose and Use Limitation Risk:

Privacy Risk: There is a potential risk that PII maintained in the system could be used or accessed inappropriately.

Mitigation: This risk is mitigated by limiting FAMS user access to only that information for which there is a business need, which is facilitated through the use of FAMS role-based access. This risk is further mitigated by FDIC policies and procedures regarding the appropriate handling of sensitive information, including PII, procurement and contract information. Additionally, FAMS training courses/sessions will include information that addresses the collection, maintenance and protection of PII in conjunction with the procurement and contracting function.

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?

<table>
<thead>
<tr>
<th>PII Element</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Name</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Date of Birth</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Place of Birth</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Social Security Number</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Employment Status, History or Information</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Mother’s Maiden Name</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Certificates (e.g., birth, death, naturalization, marriage, etc.)</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Medical Information (Medical Records Numbers, Medical Notes, or X-rays)</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Home Address</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Phone Number(s)</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Email Address</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Employee Identification Number (EIN)</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.) Potentially, in instances where a vendor is a sole proprietor.</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Driver’s License/State Identification Number</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Vehicle Identifiers (e.g., license plates)</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Education Records</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Criminal Information</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Military Status and/or Records</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Investigation Report or Database (Potentially key personnel background investigation information)</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Biometric Identifiers (e.g., fingerprint, voiceprint)</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Photographic Identifiers (e.g., image, x-ray, video)</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Other (Specify: <em>FDIC Network ID</em>_____________________________________)</td>
<td>×</td>
<td></td>
</tr>
</tbody>
</table>
1.2 Who/what are the sources of the PII in the information system or project?

<table>
<thead>
<tr>
<th>Data Source</th>
<th>Description of Information Provided by Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAMS Users</td>
<td>FAMS users may receive information from vendors external to FAMS (e.g., US Mail, email or FedConnect) and then upload or transcribe the information to FAMS. The PII entered into FAMS typically includes vendor contact information, such as name, phone number, and email address. Additionally, the name, contact information, and resumes of key personnel may be included with vendor proposals.</td>
</tr>
<tr>
<td>FDIC New Financial Environment (NFE) and United States General Services Administration (GSA) System for Award Management (SAM)²</td>
<td>GSA SAM is a website maintained by the Federal Government that collects information about entities registering to do business with the Federal Government. SAM provides vendor information via a batch job to FDIC on a daily basis, where it is uploaded to FDIC’s New Financial Environment (NFE). NFE then downloads the information, which includes PII about sole proprietors, such as vendor name, banking information, Taxpayer Identification Number (TIN), and physical address, to the FDIC’s Enterprise Data Warehouse (EDW). The information in EDW is subsequently imported, with the exception of TIN, into FAMS on a nightly basis. FDIC has disabled FAMS’ capability to maintain and use TINs, since TINs can be the social security numbers of sole proprietors. A vendor code is assigned to vendors by NFE, which can then be used to identify vendors in both FAMS and NFE.</td>
</tr>
<tr>
<td>FedConnect</td>
<td>FedConnect is an online service administered and maintained by Unison that will be integrated with FAMS in future releases. Once the integration between FAMS and FedConnect is fully implemented, vendors who wish to contract with FDIC will typically be required to register with FedConnect. Once registered, they’ll be able to use FedConnect to securely send responses, which may include PII, such as contact information or information about key personnel, to FDIC solicitations via the FedConnect/FAMS integrated service. The FAMS/FedConnect integrated service will also include a secure messaging service that will allow FDIC FAMS users and vendors to exchange messages, which may include PII, via the FAMS/FedConnect integrated service.</td>
</tr>
<tr>
<td>FDIC Access Request and Certification System (ARCS)</td>
<td>FDIC user information (employee/contractor name, NTID, work telephone number, work email address) obtained from ARCS is used by FAMS administrators to manually establish user accounts in FAMS.</td>
</tr>
</tbody>
</table>

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

Yes, the system will be granted an ATO prior to use and will be periodically reviewed as part of the FDIC ongoing authorization process.

Section 2.0: Transparency

Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

2.1 How does the agency revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change?

Through the conduct, evaluation and review of PIAs, 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 GSA Privacy Impact Assessment (PIA) for System for Award Management (SAM) (July 16, 2020), https://www.gsa.gov/cdnstatic/System_for_Award_Management_(SAM)_PIA_July2020docx.pdf
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.

FAMS operates under the following SORNs:

- GSA SORN GSA/GOVT-9 System for Award Management (SAM), which provides coverage for records that capture information users voluntarily provide about their entity as part of the process to register to do business with the Federal Government via SAM.gov, including the vendor name, vendor banking information, vendor TIN, and vendor physical address. In the case of a sole proprietor, tax laws allow them to use their Social Security Number (SSN) as their TIN.

- FDIC SORN 30-64-0012, Financial Information Management Records, which provides coverage for current and former vendors and contractors providing goods and/or services to the FDIC and associated contractor, vendor, and other accounts payable records that consist of all documents relating to the purchase of goods and/or services from those individuals including contractual documents, vendor addresses and financial institution account information, vendor invoice statements; amounts paid, and vendor tax identification number. Copies of documentation supporting vendor invoice statements may contain identifying data, such as account number.

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

While FAMS is a new system, the SORNs referenced in 2.2 will not require amendment or revision. Generally, the FDIC conducts reviews of its SORNs every three years or as needed.

2.4 If a Privacy Act Statement is required, how is the Privacy Act Statement provided to individuals before collecting their PII? (The Privacy Act Statement provides formal notice to individuals of the authority to collect PII, the purpose for collection, intended uses of the information and the consequences of not providing the information.) Explain.

FAMS may be used to process, store, maintain, disseminate, or disclose information about vendors that are sole proprietors that was originally collected from GSA SAM, which operates under System of Records GSA/GOVT-9, System for Award Management (SAM). A Privacy Notice is provided to those entities during the SAM registration process. Additionally, in future releases of FAMS, vendors that want to conduct business with FDIC will typically be required to register with FedConnect. The FedConnect registration page provides users with the terms and conditions of the FedConnect system, which discusses the usage and sharing of PII that may be collected.

Additionally, The FDIC ensures that its forms, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974 and FDIC Circular 1213.01, FDIC Forms Management Program.

2.5 How does the information system or project ensure that its privacy practices are publicly available through organizational websites or otherwise? How does the information system or project ensure that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)? Explain.

The FDIC Privacy Program page contains policies and information related to SORNs, PIAs, FDIC’s Privacy Policy, and contact information for the SAOP, the Privacy Program Manager, and the Privacy Program. See [https://www.fdic.gov/policies/privacy/index.html](https://www.fdic.gov/policies/privacy/index.html).
Privacy Risk Analysis: Related to Transparency

Privacy Risk: There is a risk that individuals are not aware that their data is maintained and processed by FAMS.

Mitigation: In instances where FAMS is provided PII from non-FDIC systems or entities, including those detailed in Section 1.0, it is incumbent upon the source system or entity to provide any applicable, required notices to the individuals from whom they collected the information. Additionally, this PIA and the SORNs listed in Section 2.2 serve as notice of the Federal Government and FDIC’s uses of this PII.

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?

Vendors do not have direct access to FAMS. Instead, FAMS receives vendor information, which may include PII, via system interface or via manual entry by FDIC personnel as described in Section 1.0. Therefore, vendors should submit requests to access and amend PII to the originating source/entity that initially collected their information.

The FDIC provides individuals the ability to have access to their PII maintained in its systems of records as specified by the Privacy Act of 1974 and FDIC Circular 1360.20. Access procedures are detailed in the SORNs listed in Section 2.2 of this PIA. The FDIC publishes its SORNs on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.20. The FDIC publishes access procedures in its SORNs, which are available on the FDIC public-facing website. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

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

Vendors do not have direct access to FAMS. Instead, FAMS receives vendor information, which may include PII, via system interface or via manual entry by FDIC personnel as described in Section 1.0. Therefore, vendors should submit requests to access and amend their PII to the originating source/entity that initially collected their information as described in Section 1.0.

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 1360.20. Access procedures are detailed in the SORNs listed in Question 2.2 of this PIA. The FDIC publishes its SORNs on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.20. The FDIC publishes access procedures in its SORNs, which are available on the FDIC public-facing website. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

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

Vendors do not provide PII directly to FAMS. Instead, FAMS receives vendor information, which may include PII, via system interface or via manual entry by FDIC personnel as described in Section 1.0. In such cases, the responsibility to notify individuals falls to the systems/entities that initially collected the information. Additionally, FAMS users may contact vendors to correct and validate their information. Further, the procedures for amending PII are published in the SORNs listed in Section 2.2 of this PIA.
Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: In some cases, FAMS is provided vendor information, including PII, from a third-party source, as described in Section 1.0. The FDIC has limited ability to implement procedures to correct inaccurate or erroneous information in such cases.

Mitigation: Vendors do not provide PII directly to FAMS. Instead, FAMS receives vendor information, which may include PII, via system interface or via manual entry by FDIC personnel as described in Section 1.0. In such cases, the responsibility to notify individuals about how to access and amend their information falls to the systems/entities that initially collected the information. Additionally, FDIC FAMS users may contact vendors to correct and validate their information. Further, the procedures for amending PII are published in the SORNs listed in Section 2.2 of this PIA.

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 Section 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 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 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 FAMS are captured in this PIA, which was conducted in accordance with applicable law, OMB policy, and FDIC policy (Circular 1360.20). PIAs are posted on FDIC’s public-facing website, [https://www.fdic.gov/policies/privacy/index.html](https://www.fdic.gov/policies/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 may be responsible for configuring, operating, troubleshooting, applying corrections, and implementing enhancements for/to FAMS based on evolving business requirements and the discovery of security vulnerabilities and system functionality defects.

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 Agreements/Non-Disclosure Agreements have been completed and signed for contractors who work on FAMS. 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, 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.**

FAMS users will be provided training when they are initially provided access to FAMS. Additionally, FAMS refresher courses will be provided on a periodic basis. The training will include information that addresses the collection, maintenance and protection of PII in conjunction with the procurement and contracting function.

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 Section 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; weekly reports to the CISO, monthly meetings with the SAOP and CISO; and Information Security Manager’s Monthly meetings.

4.9 Explain how this information system or project protects privacy by automating privacy controls?

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. Additionally, FDIC has implemented technologies to track and manage PII inventory, as well as to track, respond, remediate and report on breaches. Breaches are handled in accord with FDIC’s Breach Response Plan.

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 records under its control, as mandated by the Privacy Act of 1974 and FDIC Circular 1360.20. Disclosures are tracked and managed using FDIC’s Freedom of Information Act solution.

4.11 Explain how the information system or project retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer?

The FDIC retains the accounting of disclosures as specified by the Privacy Act of 1974 and FDIC Circular 1360.20.

4.12 Explain how the information system or project makes the accounting of disclosures available to the person named in the record upon request?

The FDIC makes the accounting of disclosures available to the person named in the record upon request as specified by the Privacy Act of 1974 and FDIC Circular 1360.20.

**Privacy Risk Analysis: Related to Accountability**

**Privacy Risk:** There are no identifiable risks associated with accountability for FAMS.

**Mitigation:** No mitigation actions are recommended.

---

**Section 5.0: Authority**

*Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.*

5.1 Provide the legal authority that permits the creation, collection, use, processing, storage, maintenance, dissemination, disclosure and/or disposing of PII within the information system or project. For example, Section 9 of the Federal Deposit Insurance Act (12 U.S.C. 1819).
The FDIC ensures that collections of PII are legally authorized through the conduct and documentation of PIAs and the development and review of 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:

- 12 USC 1819 states that FDIC can make contracts and that FDIC can make examinations of and to require information and reports from depository institutions.
- 12 CFR 366 addresses the minimum standards of integrity and fitness for an FDIC contractor.
- 12 USC 1820 discusses examinations and the authority of FDIC to make and keep copies of information for FDIC’s use.
- 12 USC 1821 deals with Deposit Insurance, the Deposit Insurance Fund and closing and resolving banks.
- 12 USC 1822 deals with FDIC as a receiver of failed banks.

**Privacy Risk Analysis: Related to Authority**

**Privacy Risk:** There are no identifiable risks associated with authority for FAMS.

**Mitigation:** No mitigation actions are recommended.

---

**Section 6.0: Minimization**

*Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.*

6.1 **How does the information system or project ensure that it has identified the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection?**

The PII elements maintained, transmitted, or shared using FAMS are restricted to those that are relevant and necessary to support FDIC’s procurement and contracting function.

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 PII elements maintained, transmitted, or shared using FAMS are restricted to those that are relevant and necessary to support FDIC’s procurement and contracting function. FAMS follows an approved record retention schedule for the collection, retention and disposal of FAMS records, which may contain PII. FAMS users will be provided with training when they are initially provided access to FAMS. Additionally, periodic FAMS refresher courses will be provided on a periodic basis. The FAMS training courses/sessions will include information that addresses the collection, maintenance and protection of PII in conjunction with the procurement and contracting function.

Annual Information 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, including minimizing the collection of PII and retention of PII.

---

7 Privacy artifacts include Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), and System of Records Notices (SORNs).
Additionally, through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that the collection and retention of PII is limited to the PII that has been legally authorized to collect.

6.3 How often does the information system or project evaluate the PII holding contained in the information system or project to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose?

FDIC maintains an inventory of systems that contain PII. On an annual basis, FDIC does an evaluation of information in the system to ensure it is the same as in the PIA and not kept longer than its retention period. New collections are evaluated to see if they are part of the inventory.

6.4 What are the retention periods of data in this information system? or project? What are the procedures for disposition of the data at the end of the retention period? Under what guidelines are the retention and disposition procedures determined? Explain.

FDIC records are retained in accordance with FDIC Circular 1210.01, FDIC Records and Information Management Program, which is informed by the Federal Records Act and NARA regulations. The retention periods and disposition procedures for records in FAMS are covered by FDIC Records Retention Schedule EIS1035, Automated Procurement System, and EIS1010, Contract Electronic File, which stipulates the following:

- Contract management/procurement data, including contractor name/type/award number, Minority and Women Owned Business information, expenditures, award value, closeout date, Contracting Officer, and Oversight Manager should be destroyed/deleted 20 years after the award effective date, provided the award has been closed out.

- Contractor Performance Evaluations, solicitations, awards, modification documents; OM/Technical Monitor appointment memos, and solicitation milestone schedules should be destroyed/deleted seven years after contract closeout.

- Cancelled solicitations and draft awards should be destroyed/deleted one year after they are cancelled.

- Newsfeeds/Announcements, bulletins that announce system releases, system offline maintenance notifications, COs tips/reminders, etc. should be destroyed/deleted when superseded, obsolete, or no longer needed.

- Pre-Award and Pre-solicitation documentation, including Requests for Proposals, Requests for Quotations, Requests for Task Order Proposals, amendments, proposals; evaluation documents, and selection approval documents should be destroyed/deleted seven years after the close of the contract.

- Post Award information, including contracts, modifications; oversight manager and technical monitors nomination documentation; other contact administration documents, and correspondence should be destroyed/deleted seven years after the close of the contract.

- Oversight Manager file information, including invoice related documents, deliverables, tracking of contractor personnel, tracking of FDIC-furnished property, and performance documentation should be destroyed/deleted seven years after the close of the contract.
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?

PII maintained, transmitted or shared by FAMS is not used for testing, training, or research unless appropriately authorized. The FDIC is in the process of developing an enterprise test data strategy to reinforce the need to mask or utilize synthetic data in the lower environments whenever possible, and ensure all environments are secured appropriately based on the impact level of the information and the information system. Additionally, the project team is required to consult with the FDIC Privacy Section to identify PII and ensure it is adequately protected or transformed before it is used in test or lower environments.

Privacy Risk Analysis: Related to Minimization

Privacy Risk: There is a risk that the personally identifiable information maintained by FAMS may be unnecessary or excessive, or may be kept longer than is necessary to meet the business need for which it was collected.

Mitigation: This risk is mitigated by FDIC policy regarding the collection, use, and retention of FAMS records and FAMS users being appropriately trained. FAMS follows an approved record retention schedule for the collection, retention and disposal of FAMS records, which may contain PII. FAMS users will be provided training when they are initially provided access to FAMS. Additionally, FAMS refresher courses will be provided on a periodic basis. The FAMS training courses/sessions will include information that addresses the collection, maintenance and protection of PII in conjunction with the procurement and contracting function.

Privacy Risk: There is a potential risk that FAMS information, including PII, could be used in test or lower environments beyond that which is necessary.

Mitigation: The FDIC is in the process of developing an enterprise test data strategy to mask or utilize synthetic data in the test and lower environments whenever possible, and to ensure all environments are secured appropriately based on the impact level of the information and the information system.

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.

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.

FAMS receives vendor information, which may include PII, via system interface or via manual entry by FDIC personnel as described in Section 1.0. In instances where information is manually entered to FAMS, FAMS users review PII contained within the records prior to the records being uploaded to FAMS to ensure that the information is accurate, relevant, timely, and complete. Additionally, FDIC relies upon GSA SAM, as well as the vendors conducting business with FDIC, to provide FDIC with data that is accurate, relevant, timely, and complete.

FAMS users will be provided FAMS training when they are initially provided access to FAMS. Additionally, periodic refresher courses will be provided on a periodic basis. The training courses/sessions will include information that addresses the collection, maintenance and protection of PII in conjunction with the procurement and contracting function.

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?

FAMS does not collect PII directly from vendors, but instead receives information, which may include PII, via system interface or via manual entry as described in Section 1.0.

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

FAMS receives vendor information, which may include PII, via system interface or via manual entry by FDIC FAMS users as described in Section 1.0. In instances where information is manually entered to FAMS, FAMS users review PII contained within records prior to the records being uploaded to FAMS to ensure that the information is correct and current. Additionally, FDIC relies upon GSA SAM, as well as the vendors conducting business with FDIC, to provide FDIC with vendor data that is current and accurate. Also, as noted in the response to Question 6.4, FDIC records are retained in accordance with the FDIC Circular 1210.01, FDIC Records and Information Management Program, which is informed by the Federal Records Act and NARA regulations, and which reduces the risk for the maintenance of outdated information.

Further, the FDIC reviews privacy artifacts to ensure adequate measures are in place 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 PII. The Office of the Chief Information Security Officer validates the configuration of administrative and technical controls for the system based on the FIPS 199 determination.

7.6 Does this information system or project necessitate the establishment of a Data Integrity Board to oversee a Computer Matching Agreements and ensure that such an agreement complies with the computer matching provisions of the Privacy Act?

The FDIC does not maintain any Computer Matching Agreements under the Privacy Act of 1974, as amended, by the Computer Matching and Privacy Protection Act of 1988, and consequently does not have a need to establish a Data Integrity Board.

**Privacy Risk Analysis: Related to Data Quality and Integrity**

**Privacy Risk:** There is a potential risk associated with data quality and integrity because vendor information may be manually entered into FAMS by FAMS users.

**Mitigation:** This risk is mitigated by FAMS users being appropriately trained and by FAMS users reviewing PII contained within records prior to the records being uploaded to FAMS to ensure that the information is correct and current.
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.

FAMS does not collect PII directly from individuals, however, FAMS may be used to process, store, maintain, disseminate, or disclose information about vendors that was originally collected from GSA SAM, which operates under System of Records GSA/GOV'T-9, System for Award Management. A Privacy Notice is provided to those entities during the SAM registration process. Additionally, in future releases of FAMS, vendors may provide information that includes PII to FDIC via FedConnect. The FedConnect registration page provides users with the terms and conditions of the FedConnect system, which discuss the usage and sharing of PII that may be collected. Further, this PIA and the SORNs listed under Question 2.2 serve as notice of the information collection.

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.

FAMS does not collect PII directly from individuals, however, FAMS may be used to process, store, maintain, disseminate, or disclose information about vendors that are sole proprietors that was originally collected from GSA SAM, which operates under System of Records GSA/GOV'T-9 System for Award Management. A Privacy Notice is provided to those entities during the SAM registration process. Additionally, in future releases of FAMS, vendors may provide information that includes PII to FDIC via FedConnect. The FedConnect registration page provides users with the terms and conditions of the FedConnect system, which discuss the usage and sharing of PII that may be collected. Further, this PIA and the SORNs listed in Question 2.2 serve as notice and implicit consent with respect to the collection, use, and disclosure of PII.

8.3 Explain how the information system or project obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII.

It is not feasible or appropriate to get direct consent prior to any new use or disclosures of previously collected PII. If applicable, the FDIC Privacy Program will update the relevant FDIC Privacy Act SORNs, 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.

FAMS does not collect PII directly from individuals, however, FAMS may be used to process, store, maintain, disseminate, or disclose information about vendors that are sole proprietors that was originally collected from GSA SAM, which operates under System of Records GSA/GOV'T-9 System for Award Management. A Privacy Notice is provided to those entities during the SAM registration process. Additionally, in future releases of FAMS, vendors may provide information that includes PII to FDIC via FedConnect. The FedConnect registration page provides users with the terms and conditions of the FedConnect system, which discuss the usage and sharing of PII that may be collected. If applicable, the FDIC Privacy Program will update this PIA or the relevant FDIC Privacy Act SORNs.
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/policies/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 is a risk related to individual participation for FAMS because data is not always collected directly from individuals. Instead, FAMS typically receives PII via the system interface or the entities described in Section 1.0 of this PIA. Therefore, individuals may not be aware and/or have provided explicit consent for the collection and use of their information within FAMS.

Mitigation: In instances where FAMS obtains PII from a third-party source, as described in the first section of this PIA, the FDIC does not have the ability to provide privacy notices or obtain explicit consent prior to its processing of these individuals’ PII. It is incumbent upon the source system or entity to provide any applicable, required notices to the individuals from whom they collected the information. Individuals should review the relevant third party’s privacy notices. Additionally, this PIA and the SORNs listed in Section 2.2 serve as notice and implicit consent with respect to the collection, use, and disclosure of PII.

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.

Acquisition-related information, including PII, is collected and maintained in FAMS and may be used throughout the various phases of the acquisition life cycle, in conjunction with FDIC’s insurer, supervision, examination, and resolution responsibilities set forth in 12 U.S.C. 1819, 12 U.S.C. 1820, 12 U.S.C. 1821, and 12 U.S.C. 1822. The information collected, maintained and used by FAMS is necessary to accurately document, award, manage, and administer procurement actions.

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.

Access to all FAMS information is based on a business need to know and the principle of least privilege. Users of FAMS are responsible for assuring proper use of the data in FAMS and, if applicable, for determining what data can be shared with other parties.

Additionally, through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that PII is only used for authorized purposes 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.

Access to FAMS is controlled via FDIC single sign on, which authenticates user account credentials via FDIC’s Active Directory. As such, FAMS users must be active users on FDIC’s network. Information within FAMS is dependent upon a person’s need to know and the principle of least privilege. The FDIC’s Access Request and Certification System (ARCS) is used to facilitate the tracking and management of FDIC employees that are FAMS users.

ARCS requests must be submitted by users and approved by managers in order to gain access to FAMS. User access is further controlled and restricted according to specific user and administrative roles that have been defined and established within FAMS, and which are based on the functions needed to perform specific jobs.

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.

On a nightly basis, FAMS exports all data changes made to FAMS during the day to the FDIC Enterprise Data Warehouse (EDW) and also synchronizes expenditure, requisition and vendor information data with the FDIC EDW Enterprise Operation Data Store (ENTODS). Acquisition and contract information is then uploaded from EDW ENTODS to FDIC’s New Financial Environment via a nightly batch job.

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, FAMS does not aggregate or consolidate data in order to make determinations or derive new data about individuals.

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.

In future releases of FAMS, FAMS will share data with Unison’s FedConnect service through an interface module that is installed in the FAMS environment. Vendors who want to work with FDIC will typically be required to register with FedConnect. FedConnect can be used by FAMS users to post solicitation documents to the FedConnect vendor/applicant community, communicate with vendors/applicants, and retrieve responses from the vendor/applicant community. Only FAMS will be able to initiate a communication with FedConnect, and FAMS users will only be able to exchange messages via FedConnect with the vendors that are associated with the particular solicitation/contract on which a FAMS user is currently working. The vendor will need to be associated with the solicitation/contract in FAMS in order for a message or information to be sent to them by a FAMS user.

Through the conduct, evaluation and review of PIAs and SORNs, the FDIC ensures that PII shared with third parties is used only for the authorized purposes identified or for a purpose compatible with those purposes, in accordance with the Privacy Act of 1974, FDIC Circular 1360.20, FDIC Privacy Program, and FDIC Circular 1360.17, Information Technology Security Guidance for FDIC Procurements/Third Party Products. The FDIC also ensures that agreements regarding the sharing of PII with third parties specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used, in accordance with FDIC Circular 1360.17 and FDIC Circular 1360.9.
9.7 Describe how the information system or project monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII.

FAMS users will be provided training when they are initially provided access to FAMS. Additionally, periodic refresher courses will be provided on a periodic basis. The training courses/sessions will include information that addresses the collection, maintenance and protection of PII in conjunction with the procurement and contracting function.

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 Purpose and Use Limitation**

**Privacy Risk:** There is a potential risk that PII maintained in FAMS could be used or accessed inappropriately.

**Mitigation:** This risk is mitigated by limiting FAMS user access to only that information for which there is a business need, which is facilitated through the use of FAMS role-based access. This risk is further mitigated by FDIC policies and procedures regarding the appropriate handling of sensitive information, including PII, procurement and contract information. Additionally, the FAMS training courses/sessions will include information that addresses the collection, maintenance and protection of PII in conjunction with the procurement and contracting function.

---

**Section 10.0: Security**

*A agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.*

10.1 Describe the process that establishes, maintains, and updates an inventory that contains a listing of all information systems or projects identified as collecting, using, maintaining, or sharing personally identifiable information (PII).

FDIC maintains an inventory of systems that contain PII. On a semi-annual basis, FDIC does an evaluation of information in the system to ensure it is the same as in the PIA and not kept longer than its retention period. New collections are evaluated to see if they are part of the inventory.

10.2 Describe the process that provides each update of the PII inventory to the CIO or information security official to support the establishment of information security requirements for all new or modified information systems or projects containing PII?

The FDIC Privacy Program updates the Chief Information Security Officer (CISO) on PII holdings via the PTA adjudication process. As part of the PTA adjudication process, the FDIC Privacy Program reviews the system or project’s FIPS 199 determination. The FDIC Privacy Program will recommend the appropriate determination to the CISO should the potential loss of confidentiality be expected to cause a serious adverse effect on individuals.
10.3 Has a Privacy Incident Response Plan been developed and implemented?

FDIC has developed and implemented a Breach Response Plan in accordance with OMB M-17-12.

10.4 How does the agency provide an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan?

Responses to privacy breaches are addressed in an organized and effective manner in accordance with the FDIC's Breach Response Plan.

**Privacy Risk Analysis: Related to Security**

**Privacy Risk:** There are no identifiable risks associated with security for FAMS.

**Mitigation:** No mitigation actions are recommended.