Retail Product Network
Financial Agent Selection Process

Requirements Document and
Solicitation of Services

Bureau of the Fiscal Service

June 15th, 2026

I. INTRODUCTION

The Bureau of the Fiscal Service (BFS) seeks a Financial Agent capable of providing and operating a secure, government-controlled payment and collections platform that supports retail, digital, and future payment channels through a unified transaction, reconciliation, and reporting framework. Interested financial institutions should respond with a proposal in the form specified in Section VI of this solicitation.

BFS will conduct the selection pursuant to its Financial Agent Selection Process (FASP), under authorities that include 12 U.S.C. §§ 90, 265, and 266 and 31 CFR Part 202. The financial institution selected shall be a Financial Agent (FA) of the United States and will have a fiduciary responsibility to act in the best interests of BFS, including a duty of loyalty and fair dealing. BFS will expect full transparency in all dealings with the FA, including all communications and pricing.

BFS will evaluate the proposals submitted by financial institutions in two phases. In Phase I, BFS will review all the Proposals and select up to four finalists. In Phase II, each finalist will receive additional detailed information and present their final proposal, and the Bureau of the Fiscal Service will select one of the finalists as the designated FA.

The FA may with the prior written consent of BFS contract with other service providers including non-financial institutions such as processors or financial technology companies, and other third-party contractors (individually or collectively "contractors") to assist in providing the services. The FA will have a legal relationship with BFS and liability and responsibility to BFS for any services provided by its contractors.

BFS intends to enter into a Financial Agency Agreement (FAA) with the selected FA to provide services to the Retail Product Network (RPN). The term of the FAA will commence on or about May 2027. BFS currently anticipates that the FAA will have an initial term of four (4) years, with two (2) two-year options and two (1) one-year options to be exercised at the direction and discretion of BFS. BFS does not guarantee any volumes or minimum compensation under this program.

II. BACKGROUND

BFS' mission is to drive integrity and efficiency in federal financial operations. As part of its duties, BFS operates the Treasury General Account (TGA) function as the federal government's central checking account, serving as the primary repository for all federal cash receipts and disbursements. It manages funds collected from taxes, fees, customs duties, and proceeds from U.S. government securities sales, while disbursing payments for federal obligations such as salaries, entitlement programs, and defense expenditures

On January 22, 2026, the BFS approved a strategic implementation plan, instructing the TGA team to initiate the RPN Financial Agent Selection Process (FASP). This initiative aims to establish an additional channel for supporting over-the-counter transactions AND to enable the future integration of third-party solutions, including digital payments such as stable coins.

III. OBJECTIVES

BFS is seeking a bank partner that demonstrates both the capability to fulfill key service needs and a proven willingness to collaborate with external partners and industry leaders. The ideal solution does not need to encompass all requirements internally; rather, the bank should have robust processes and partnerships in place to deliver these services seamlessly. This approach ensures access to best-in-class offerings and flexibility in meeting evolving business needs.

By holding an open competition for services, we expect to identify the most qualified FA that can provide the highest level of service at the best commercially reasonable prices. BFS is seeking one FA that can support the Retail Product Network in achieving the following business objectives:

1. Payment Acceptance
   - The solution must enable secure in-person payment of government invoices at commercial retail locations throughout the United States. Customers should be able to pay using popular methods such as major credit and debit cards.
   - The proposed solution must facilitate seamless integration with Treasury's existing settlement rails. Additionally, it should ensure a uniform customer experience while enabling BFS to exercise appropriate oversight and control regarding the design and functionality of the payment flow.
   - The solution should support the addition, removal, and management of multiple payment service providers without requiring significant changes to agency integrations.

2. Payment Transaction Management
   - The solution shall support Government-controlled payment workflows, including the ability to initiate, modify, complete, cancel, and track payment transactions. The solution should provide sufficient transaction status information to support customer service, auditability, reconciliation, and recovery from incomplete or interrupted payment flows. It also shall support integration with key federal systems responsible for capturing remittance and reconciliation elements for each payment.

3. Refund Capabilities
   - The solution shall support both full and partial refunds to the original payment method, as applicable based on the payment method used. Refund functionality should include safeguards to prevent duplicate or excessive refunds and should allow the Government to track refund status for reconciliation and customer support purposes.

4. Saved Payment Methods
   - The solution should allow customers, on an opt-in basis, to save eligible payment methods for future use. Customers should be able to manage saved payment methods, including selecting a default payment method and removing saved methods. The solution should support future payments using saved payment methods while complying with applicable payment security, authentication, privacy, and regulatory requirements.

5. Event Notifications
   - The solution shall provide timely, secure notifications or equivalent mechanisms to inform the Government of key payment events, such as successful payments, failed payments, completed refunds, failed refunds, and changes to saved payment methods. These notifications should include sufficient information to support reconciliation, audit, and operational follow-up.

6. Financial Data and Invoice Support
   - Although invoice generation and financial records will be maintained by the Government, the solution shall provide transaction-level and line-item-level payment data needed to support agency invoicing, accounting, audit, and reporting processes. This includes support for individual charges, fees, adjustments, and other payment-related financial details.

7. Reconciliation and Recovery
   - The solution shall provide the Government with the ability to retrieve payment, refund, and checkout-related transaction information when needed. These capabilities should support manual reconciliation, investigation of discrepancies, recovery from missed notifications, and customer service inquiries.

8. Currency and Pricing
   - The solution shall support payments in U.S. dollars and provide sufficient pricing detail to support line-item-level accounting rather than only aggregate transaction totals.
   - The solution may also support future payment methods, including stable coin-based payment options, provided that settlement, reporting, reconciliation, refund handling, and accounting treatment can be supported in a manner acceptable to the Government and consistent with applicable requirements.

9. Availability and Performance
   - The solution shall provide high availability appropriate for mission-facing Federal services and shall process payments within commercially reasonable timeframes under normal operating conditions. The provider should describe its service availability commitments, performance expectations, monitoring practices, and incident response approach.

As a part of the formulation of this recommendation, the following goals and risks were considered:

- **Market availability**: Use, when available, off-the-shelf options that can be quickly adopted and implemented yet will meet the security requirements of BFS;
- **Stable, secure, scalable**: Any system or service selected must meet all applicable security requirements;
- **Funds Security:** Provide adequate collateralization for public funds held by the FA;
- **Innovation for the Future:** This new channel must support over the counter transactions and provide the opportunity to implement any third-party solution in the future. BFS is continuously seeking improvements and innovations to reduce check volumes. The FA should provide its operational expertise, innovation capabilities, industry knowledge, and fiduciary guidance to assist BFS in this respect.

IV. TECHNICAL AND PROGRAM REQUIREMENTS

A. The Basic Process Flow

As currently envisioned, BFS seeks proposals to facilitate the following transaction flow:

1. Consumer receives a bill from an agency and takes the bill to a retail partner of their choice;
2. Consumer presents the bill/account number and pays with cash, money order, or card (future iterations should be able to accept digital payments such as stable coins);
3. Consumer receives a receipt with transaction details;
4. Financial management and risk management software tools send payment information back to the agency which includes a real-time API call or an end-of-day batch file with transaction information to complete transaction and credit customer's account.

The financial institution will assume custodial responsibilities for administering, safeguarding, assessing, and executing payments utilizing a secure advance-payment protocol on behalf of BFS. All payment transactions shall be processed in accordance with established standard procedures.

BFS will serve as the primary customer for the services provided. Federal agencies will engage directly with the financial institution's payment process network to facilitate transactions and manage payments. BFS will coordinate with the designated point of contact or program manager within the FA's payment processing network. This relationship encompasses both administrative and financial responsibilities, with back-office duties focused on supervising and managing the bank's process network.

Within the proposal, the financial institution must provide a plan describing how its solution will be implemented no later than May 27th, 2027. The FA should provide an Implementation model including expertise of any contractors.

1. The financial institution must describe how its RPN solution will meet the requirements as described in the objectives:
   - The solution should support several payment methods. Please describe which types can be accommodated; at a minimum - cash, money order, and card must be included and provide the capabilities to adopt alternative payment solutions in the future (i.e., stable coin-based payments, etc.).
   - All payments must be received and returned in US dollars.
   - The Agent has a fiduciary responsibility to ensure proper internal controls are in place to secure and account for all incoming payments.
   - Provide a unique payment confirmation to the payer upon successful completion of payment.
   - Establish connections via API with BFS to:
     - Validate data in real time
     - Send notification that payment has been posted
     - Explain what services are being proposed with associated timeline.
   - Provide customer service support to federal agencies and payers. Hours of support are from 8am EST to 8pm EST.

2. The financial institution must describe how security requirements of the RPN solution will

be met and managed, and how the platform will be stable and resilient, as follows:

- Support FISMA moderate and build in zero-trust architecture.
- Maintain a FedRAMP moderate environment, or equivalent, with corresponding Treasury policies.
- Describe experience in the last five years in supporting government clients to secure and manage Privacy Act and Federal Tax Information data. Should include size, scope and complexity of experience.
- Describe how the RPN will keep costs low, manage operational costs, and ensure the lowest budgetary impact to the public using the categories of Implementation, Development, Configuration, Deployment, Ongoing Maintenance and Operational costs.
- Clearly articulate the innovations they intend to propose to promote greater adoption of electronic services.
- Clearly detail proposed services, explain their relevance to BFS's needs, and provide a transparent timeline for completion.
- Describe plans to ensure resiliency and contingency of the solution.

B. Program Resources

The FA will provide staff with expertise in all aspects of incoming payments, collateral management, profile management and role access, project management, customer service, change requests, security and fraud monitoring, and technical innovation.

C. Service level Agreements

The FA will provide the highest standards of performance and quality and must perform ongoing quality assurance and quality control reviews. BFS will review the established quality controls and quality control reviews on an ongoing basis to ensure performance meets established standards. This review will include accuracy, resource effort, volume accountability, processing times, workload tracking, management responsiveness, security, and service availability.

D. Operating Schedule

General production hours of operation will be 24/7/365. Customer service support should be provided focused solely on how to make payments. Hours of support should be from 8am EST to 8pm EST weekdays. The solution may have daily maintenance and batch processing windows, including start-of-day and end-of-day activities.

E. Relationship Management

The FA will maintain service representatives who are knowledgeable about BFS' specific program needs and requirements and are available to provide support as needed.

F. Monthly Expense Reporting

The FA will use BFS' Bank Management System (BMS) for reporting monthly expenses and other program data. BMS is a web-based system and does not require an established system-to-system interface. It accepts both file uploads and manual entry of compensation requests.

G. Security and certification Requirements (Please See Attachment A)

In addition to the security-related objectives and technical and program requirements described above, the FA must comply with BFS' security framework for the Retail Product Network solution, as follows:

- The FA will meet and adhere to all applicable federal security requirements listed in Attachment A, including all federal government requirements for (1) physical and personnel security, (2) information technology security and privacy controls, and (3) disaster recovery and continuity of operations.
- The FA will assist with BFS security reviews or audits by providing information about processes, software, facilities, personnel, equipment, and security and privacy controls through interviews, on-site inspections, and documentary evidence, and assist as otherwise directed.
- The FA must ensure all employees and all contractors working on the Retail Product Solution are citizens or lawful permanent residents of the United States. All facilities and systems used to provide support for the Retail Product Solution must be located in the United States.
- The FA must confirm that it will not use covered telecommunications equipment or services, as defined in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232, § 889), as a substantial or essential component of the services provided, or as critical technology as part of the services provided.

H. Audit and Record Retention

The FA will assist BFS with any audits or other reviews and retain all records, reports, documents, and other evidence related to the performance of its account verification services in accordance with government retention schedules.

V. OVERALL FASP FORMAT

The Retail Product Network FASP will be broken into two phases. The first phase will focus on the solution being offered, the financial institution's experience and capability to deliver the retail product services to scale, commitment to follow BFS Security Requirements, recommendations for innovation and enhancement, commitment to sign the core Financial Agency Agreement (FAA), rationale and explanation for the proposed Retail Product technology, and redundancy.

Following the written Phase I proposal, each financial institution will be scheduled for an in-person briefing covering the contents of their proposal. The oral presentation/briefing will provide an opportunity for us to ask questions and ensure there is no miscommunication or misunderstanding regarding the written proposal.

- Evaluation criteria will consist of: Processing Capability & Experience
- Technology, redundancy, & Customer access to payment locations

The second phase will also require a written proposal which will focus on pricing, the ability and plan to

control costs and drive efficiencies. Like Phase I, each financial institution will be scheduled for an in-person briefing covering the contents of their Phase II proposals. The oral presentation/briefing will provide an opportunity for us to ask questions and ensure there is no miscommunication or misunderstanding regarding the written proposal.

- Implementation Plan
- Efficiencies, Innovation, & Cost Management
- Pricing

Prior to each phase, BFS will host an information session to provide more details and answer questions.

VI. PRE-FASP

For those financial institutions interested in responding, the pre-FASP requirements are:

- Submit a letter of intent to respond to the RPN FASP on official letterhead signed by the appropriate officer of your bank.
- Along with the above letter, please provide signed Non-Disclosure Agreements (NDA) for those in your organization that will be working to respond to the RPN FASP (See Appendix XIII for the NDA).
- Respond to the initial Information Session to RPNFASP@fiscal.treasury.gov. A maximum of 4 representatives will be accepted from each financial institution. Signed NDAs will be required for the Information Session.
- Phase I Information Session: An information session will be held virtually on June 25th, 2026, starting at 9:30am. The session will cover a summary of the entire FASP, and we will provide detailed information on requirements for Phase I proposals including specifics surrounding security and audit requirements, the core Financial Agency Agreement (FAA), how to interface with BMS, and Statements of Required Services. Details regarding in-person briefings on proposals will be covered at the information session.

VII. RESPONSES FOR PHASE I

Proposal Format Requirements

Proposal documents should not be marked as *"Proprietary and Confidential"* and BFS will not honor any such markings. However, because Proposals may be subject to Freedom of Information Act (FOIA) requests, Congressional inquiries, or other requests, Proposal documents may be labelled as *"Program Sensitive"* to emphasize concerns about the disclosure of confidential business information.

Proposals should not contain, and the BFS will not consider, information on pricing and program costs. BFS will request pricing information from finalists in Phase II of the evaluation process.

Format Specifications: Proposals must be formatted as follows:

- No more than 20 one-sided pages (not including any requested attachments)
- Appendix - no more than 10 pages
- Paper size 8 ½" x 11"
- Single-spaced
- Font type and size – 12-point Times New Roman font
- Margin size – one inch
- The table of contents is optional (not included in maximum 20-page)
- Adobe PDF format of the proposal and transmittal letter

Transmittal Letter: Proposals must include a transmittal letter as follows:

- The transmittal letter must be written on the financial institution's letterhead and be signed by an official of the financial institution with legal authority to represent and bind the institution.
- The transmittal letter must include the name, title, mailing address, e-mail address, and telephone number of the financial institution's contact person for all communications related to the FASP.
- The financial institution must affirmatively state in the transmittal letter that it (1) qualifies as a financial agent under 31 CFR Part 202; (2) agrees to the selection and evaluation approach described in this solicitation; and (3) understands that the selection is subject to the BFS's FASP and is not subject to the Federal Acquisition Regulation (FAR).

Submission: Financial institutions should submit their PDF formatted response to RPNFASP@fiscal.treasury.gov by **5:00 pm ET on August 3rd, 2026**.

Questions about the Solicitation: Outside of the information sessions, financial institutions should direct all questions about this solicitation to the following email mailbox address: RPNFASP@fiscal.treasury.gov. BFS will respond to all questions in writing via e-mail as soon as possible and may share questions and answers with other respondent financial institutions.

Phase I Proposal Details

The first phase will focus on the financial institution's experience and capability to deliver the retail product services to scale, commitment to follow BFS Security Requirements, recommendations for innovation and enhancement, commitment to sign the core Financial Agency Agreement (FAA), rationale and explanation for the proposed Retail Product technology, and redundancy.

Proposals should clearly demonstrate the financial institution's ability to meet the related Objectives in Section B., along with the ability to address requirements in Section IV, *Technical and Processing Requirements.* At a minimum, Phase I proposals should describe the following:

- Experience, both corporate and staff that will be assigned;
- Explanation regarding staffing methodology (temporary vs permanent) and how those positions will be filled;
- Plan to meet customer service requirements;

- Plan on how this solution will over the counter transactions and provide the opportunity to implement any third-party solution in the future;
- Rationale for proposed technology and equipment platforms;
- Plans for redundancy and disaster recovery including recovery times;
- Commitments to follow Bureau security requirements;
- Commitments to interface with potential BFS systems to include BMS;
- Commitment to terms in the core FAA; and
- Any other relevant information to assist BFS in evaluating the Phase I proposal.

VIII. PHASE I EVALUATION AND SCORING

After all of the submitting financial institutions' in-person briefings are completed, BFS will evaluate and score all Phase I proposals and invite up to four (4) financial institutions with the highest scores to proceed to Phase II as finalists. The selection of those highest scoring proposals is at the sole discretion of BFS. BFS will notify those financial institutions below the top 4 scores that they will not be moving on to Phase II of the FASP.

IX. PHASE II INFORMATION

BFS will conduct a Phase II information session for all finalists. The Phase II session will provide detailed information regarding information and materials regarding the pricing template, transition plan, and efficiency and cost management requirements, along with how to respond with Phase II proposals.

Additional information sessions consisting of open dialogue with BFS, both with individual finalists and collectively with all finalists, may occur at the discretion of BFS. BFS will provide all finalists with the opportunity to ask questions and to clarify the terms of their Proposals throughout the evaluation process.

Each finalist will be invited to present its final Phase II Proposal in an oral presentation held in person at BFS headquarters in Washington, DC. After the oral presentations, BFS will select one finalist as the FA for the RPN. The FA will be required to execute the FAA with BFS within approximately 3 months after the date it is notified of its selection.

X. FASP TIMELINE

The table below is the current timeline. Please note that while we will make our best efforts to adhere to these dates, there may be circumstances that force date changes.

RPN FASP Event	EXPECTED START	EXPECTED END
Publish RPN FASP	6/15/2026	6/15/2026
Provide Q&A responses from interested FIs	6/16/2026	7/24/2026
RPN FASP Information Session	6/25/2026	6/25/2026

Phase I Proposals Due	8/3/2026	8/3/2026
Score Phase I	8/5/2026	8/17/2026
Phase I Oral Presentations - 1-2 weeks	8/24/2026	9/8/2026
Notify FIs - Non-Selection or Advance to Phase II, Provide Phase II .Documentation	9/15/2026	9/15/2026
Phase II Information Session	9/22/2026	9/22/2026
Phase II Proposals Due	10/6/2026	10/6/2026
Phase II Oral Presentations	10/13/2026	10/16/2026
Final Negotiations - 4 weeks	12/3/2026	1/14/2027
Sign FAA	**1/14/2027**	**1/21/2027**

This financial agent solicitation may be amended from time to time, or cancelled in its entirety, in the sole discretion of BFS.

XI. APPENDIX

- Non-Disclosure Form
- Attachment A

XII. APPENDIX

NON-DISCLOSURE AGREEMENT
Between
U.S. Department of the Treasury, Bureau of the Fiscal Service,
and

WHEREAS, the U.S. Department of the Treasury, Bureau of the Fiscal Service ("BFS") is currently soliciting proposals from commercial banks for the operation of a Retail Product Network;

WHEREAS, _____ ("Bank") has expressed a prospective interest to BFS in participating in the Retail Product Network Financial Agent Selection Process ("FASP"), and BFS deems it to be in the Government's best interest to facilitate receipt of a proposal from Bank in connection with the Retail Product Network FASP, because increased competition enhances the probability of BFS selecting an agent whose proposal best meets the Government's needs;

WHEREAS, Bank may, in order to most effectively participate in the RPN FASP require, at the sole discretion of BFS, access to certain Confidential Information of BFS for use in connection with the preparation of its proposal;

NOW, THEREFORE, in consideration of the foregoing, and the mutual promises and covenants contained herein, the receipt and sufficiency of which are hereby acknowledged, BFS and Bank hereby enter into this Non-Disclosure Agreement ("Agreement"), subject to the following terms and conditions:

1. **Confidential Information.** BFS may, in its sole discretion, disclose to Bank the following documents and information about the BFS applications, which constitute Confidential Information: source code, documentation such as use cases, screen prints, details of interfaces, application architecture, security, operating procedures, authentication and authorization approaches for Retail Product Network or Confidential information deemed necessary to disclose during discussions.

   The term "source code" means the complete version of the source codes for current BFS applications and will include all existing associated material required to enable a reasonably skilled programmer to understand the licensed product's design, structure and implementation. Additional information may include flow charts, system documentation, program procedures (including build procedures), custom or special compiler information and other material related to the structure and implementation of the systems.

2. **No Representation as to Future Work.** Bank expressly acknowledges that it may not be selected as the financial agent pursuant to the Retail Product Network FASP, and that any costs or expenses incurred by it in preparing a proposal shall be

borne solely by Bank and are not reimbursable. The execution of this NDA does not guarantee or imply that any such work will be awarded. In addition, the requirements as outlined in the Notice to Financial Institutions, Financial Agent Selection Process for Retail Product Network remain subject to change, including cancellation without notice or cause, at any time.

3. **Duty of Confidentiality and Standard of Care.** No right, title, license, or other interest in the Confidential Information is hereby conveyed to Bank. Bank is authorized to review and use the Confidential Information for the limited purpose of developing its proposal in connection with the Retail Product Network FASP. Bank shall limit access to the Confidential Information to it and its present or prospective directors, officers, employees, agents, consultants, or advisors (collectively, "Representatives") with a need-to-know such information for the purpose of preparing its proposal for the Retail Product Network FASP. Bank and its Representatives shall not use the Confidential Information for any other purpose. This includes, but is not limited to, the use of any ideas, concepts, design and processes embodied in any Confidential Information (including but not limited to source code) provided or developing any derivative works of such Confidential Information for processing transactions for any other entity except the US Treasury. Bank agrees to take all reasonable and necessary steps to protect the confidential status of the information disclosed and agrees to use its best efforts to regain any information that has been inadvertently transmitted to a third party. Bank shall notify all employees, subsidiaries, affiliates, and Representatives to whom any of the Confidential Information is communicated or disclosed of the terms of this Agreement, and in advance of disclosure of the Confidential Information shall enter into nondisclosure agreements with such parties containing terms and conditions substantially similar to those contained herein

4. **No Warranties as to Accuracy and Completeness.** BFS makes no representation, warranty, assurance, guarantee or inducement to Bank with respect to the Confidential Information's validity, merchantability, accuracy or completeness, or to the infringement of trademarks, patents, copyrights or any other right of privacy, or other rights of third persons. Bank further agrees that BFS shall have no liability to Bank or to any of its Representatives relating to or resulting from the use of the Confidential Information by Bank or its Representatives.

5. **Equitable Relief.** Bank agrees that a breach of this Agreement would cause immediate and irreparable injury to BFS, and that money damages would not be a sufficient remedy for breach of the confidentiality obligations of this Agreement. Accordingly, BFS shall be entitled to specific performance and/or injunctive relief as a remedy for any breach of the confidentiality obligations of this Agreement. Such remedies shall not be deemed to be the exclusive remedies for a breach by Bank or its Representatives of this Agreement but shall be in addition to all other remedies available at law or equity.

6. **Return and Destruction.** Bank shall return hard copies of the Confidential Information and shall certify in writing as to the destruction of any electronic files of the Confidential Information (including without limitation all notes, extracts, studies, compilations, memoranda and other documents containing such information) to BFS

within five working days of notice of non-selection in the event that Bank is not selected to perform any work pursuant to the Retail Product Network FASP.

7. **Termination.** This Agreement shall terminate five (5) years from the effective date hereof. Any earlier termination of this Agreement shall not relieve Bank, its employees, contractors, and representatives of their obligations hereunder regarding the protection and use of Confidential Information set forth in Paragraph 3) above.

8. **Jurisdiction.** This United States District Court of the District of Columbia shall have exclusive jurisdiction and be the appropriate venue with respect to any matter relating or pertaining to this Agreement.

9. **Assignment.** This Agreement may not be assigned or otherwise transferred by Bank, in whole or in part, without the express prior written consent of BFS, which consent shall not unreasonably be withheld. This Agreement shall benefit and be binding upon the successors and assigns of the parties hereto.

10. **Paragraph Titles**. The paragraph titles contained herein shall not be deemed to be substantive and shall not be interpreted as to limit or restrict the rights and obligations of the parties as provided herein.

11. **Severability and Construction**. In the event that one or more of the provisions of this Agreement is determined to be void or unenforceable by a court of competent jurisdiction, such finding shall have no effect on the remaining provisions. If any provision is found too broad to be effective, that provision shall be limited to the minimum extent necessary and enforced to the maximum extent possible. This Agreement is a product of negotiation between the parties and expresses the mutual intent of the parties. This Agreement shall not be construed against either of the parties based on drafting.

12. **Merger.** This represents the entire Agreement of the parties concerning the exchange of the Confidential Information and supersedes any and all prior written or oral agreements thereon. It shall not be amended or modified except by subsequent agreement in writing and signed by the duly authorized representatives of the parties.

13. **Electronic Signatures**. Electronic signatures may be used in the execution of this Agreement, which, if used, shall be considered binding original signatures."

IN WITNESS WHEREOF, the undersigned represent that they are authorized to bind their respective organizations to the terms of this Agreement and hereby do so.

_____ _____

Tamara Whitaker Date
Director, Over The Counter Collection Division
Bureau of the Fiscal Service
U.S. Department of the Treasury

_____ _____

[NAME] Date
[TITLE]
[**Bank's Registered Name**]

Attachment A for FASP

1. Information Types

The term "information" is synonymous with data, regardless of format or medium.

1.1 Sensitive But Unclassified Information

Sensitive But Unclassified information (SBU) is any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy. SBU information is subject to stricter handling requirements than less sensitive non-SBU information because of the increased risk if the data are compromised. Some categories of SBU include financial, medical, health, legal, strategic, and business information. Personally Identifiable Information and Sensitive PII are also considered to be SBU. These categories of information require appropriate protection individually and may require additional protection when aggregated with other sensitive information.

1.2 Controlled Unclassified Information

CUI is defined as information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.

1.3 Personally Identifiable Information

Personally Identifiable Information (PII) as defined in OMB Memorandum M-07-16, refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to

recognize that non-PII can become PII whenever additional information that is publicly available — in any medium and from any source — is or can be combined to identify an individual. As an example, PII includes a name and an address because it uniquely identifies an individual, but alone may not constitute PII.

1.4 Sensitive Personally Identifiable Information

Sensitive PII refers to information that can be used to target, harm, or coerce an individual or entity; assume or alter an individual's or entity's identity; or alter the outcome of an individual's or entity's activities. Sensitive PII requires stricter handling because of the increased risk to an individual or associates if the information is compromised. Some categories of Sensitive PII include stand-alone information, such as Social Security numbers (SSN) or biometric identifiers. Other information such as a financial account, date of birth, maiden names, citizenship status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also considered Sensitive PII. In addition, the context of the information may determine whether it is sensitive, such as a list of employees with poor performance ratings or a list of employees who have filed a grievance or complaint.

2 Information Protection

The Financial Agent's employees, facilities, services and product(s) shall meet applicable United States (U.S.) federal government laws, directives, executive orders, standards, guidelines, and other requirements for information security, personnel security, physical security, and data encryption. The Financial Agent shall follow United States Government, Treasury, and BFS procedures for proper handling of SBU, CUI and PII. The Financial Agent may be required to assist with security reviews by providing information about processes, software, facilities, personnel, and equipment through interviews, on-site inspections (if necessary), and documentary evidence.

The Financial Agent shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed.

Security and privacy control documentation shall include an allocation of responsibility between control providers regarding control implementation. The documentation shall also include a description of the security and privacy controls implemented and demonstrated use of a system development lifecycle in the implementation of security and privacy controls. The Financial Agent shall establish processes to identify and address weaknesses or deficiencies in their supply chain. Supply chain controls will be implemented as part of these processes and documented by the Financial Agent.

The disposition of all data will be at the written direction of the BFS representative, this may include documents returned to Government control; destroyed; or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the BFS representative.

The Financial Agent shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this agreement. The Financial Agent shall also protect all Government data, equipment, etc.

Information systems and services performing work on behalf of the BFS shall be located, operated and maintained within the U.S.; operations and maintenance of systems shall be conducted by personnel physically located within the U.S or its territories. "Operated" refers to carrying out administrator/privileged user functions, such as, database administration, patching, upgrades and maintenance. Administrator/ privileged access shall not be permitted from outside of the U.S. Foreign remote maintenance, systems monitoring, foreign "call service centers," "help desks," and the like are prohibited. BFS information shall be accessed only by personnel meeting or surpassing the Treasury citizenship requirements. Extra precautions should be in place for other types of access from foreign locations.

The Financial Agent must not remove SBU, CUI or PII information from approved location(s), electronic device(s), or other container(s), without prior approval from BFS.

The Financial Agent shall report security incidents to BFS via the established incident reporting procedure in the FAA, if applicable.

2.1 Privacy Act Compliance

(a) Financial Agents must comply with the Privacy Act's requirements in the design, development, or operation of any system of records containing PII developed or operated for BFS or to accomplish a BFS function for a System of Records (SOR)[1].

(b) In the event of violations of the Act, a civil action may be brought against BFS when the violation concerns the design, development, or operation of a SOR on individuals to accomplish a BFS function, and criminal penalties may be imposed upon the officers or employees of BFS when the violation concerns the operation of a SOR on individuals to accomplish an BFS function. For purposes of the Act, when the agreement is for the operation of a SOR on individuals to accomplish a BFS function, the Financial Agent is considered to be an employee of the agency.

3 Security and Privacy Awareness Training

The Financial Agent personnel who require access to BFS information or information systems will be required to review and sign Rules of Behavior, and complete security awareness training prior to being granted access. Security and Privacy training will be required on a recurring annual basis, of all Financial Agent staff performing work for BFS on a recurring annual basis, provided by BFS and/or by the Financial Agent. Access may be revoked if the annual security training is not completed. When necessary, Financial Agents will be required to sign Non-disclosure agreements.

4 Federal Regulatory Requirements and Industry Standards

[1] "System of Records" is defined as a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

- Bureau of the Fiscal Service Baseline Security Requirements (BLSRs)
- FIPS 140, Security Requirements for Cryptographic Modules
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST Cybersecurity Framework 2.0
- NIST Privacy Framework
- NIST AI Framework
- NIST SP 800-37
- NIST SP 800-53
- NIST SP 800-53A
- NIST SP 800-63-4
- NIST SP 800-137
- NIST SP 800-171
- OMB Circular A-123
- OMB Circular A-130
- Public Law 93-579, The Privacy Act of 1974
- IRS Publication 1075
- TD P 85-01 - Treasury Information Technology Security Program
- TD P 15-71 - Department of the Treasury Security Manual
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- SSAE 18 or equivalent
- CISA Binding Operational Directives and Emergency Directives