



May 3, 2019

FINANCIAL AGENT SOLICITATION ELECTRONIC CHECK PROCESSING

I. INTRODUCTION

The Bureau of Fiscal Service (Fiscal Service) plans to select one financial institution to develop, enhance, operate and maintain the federal government's electronic check processing (ECP) revenue collection. Interested financial institutions should respond with a proposal in the form specified in Section V of this solicitation.

Fiscal Service will conduct the selection pursuant to its Financial Agent Selection Process (FASP). 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 Fiscal Service, including a duty of loyalty and fair dealing. Fiscal Service will expect full transparency in all dealings with the FA, including all communications, pricing and reporting of risk incidents.

Fiscal Service will evaluate the proposals submitted by financial institutions in up to two phases. Fiscal Service reserves the right to select an FA after Phase 1. In Phase 1, Fiscal Service will review all proposals and select up to two finalists. In Phase 2, each finalist will receive additional detailed information and present its final proposal, and Fiscal Service will select one of the finalists as FA.

Fiscal Service will enter into a five-year Financial Agency Agreement (FAA) with the FA. The term of the FAA will commence in December 2019. Fiscal Service will have the option to extend the FAA with three (3) – two (2) year extensions.

The FA may use third-party contractors to assist in providing the services required in the FAA, provided the third-party is approved by Fiscal Service. Fiscal Service encourages its FAs to use small businesses, including minority-owned or women-owned businesses, as contractors.

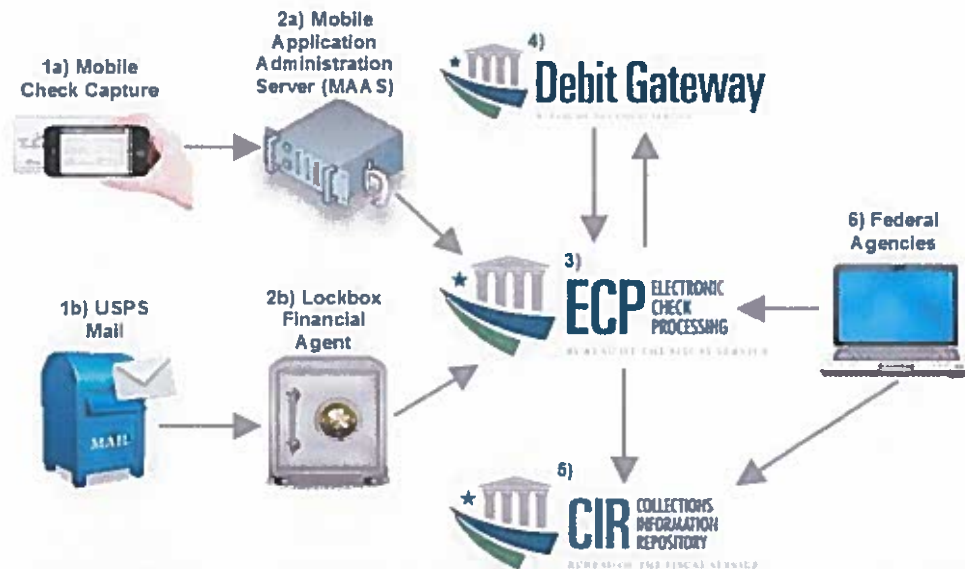
Fiscal Service encourages its FAs to participate in the voluntary Financial Agent Mentor-Protégé Program which is intended to facilitate the inclusion of a broader segment of the financial

institution community to serve as financial agents. Additional information on this Program can be found at: <https://www.fiscal.treasury.gov/files/fampp/FAMPPFlyer.pdf>

II. BACKGROUND

The Electronic Check Processing (ECP) application is a web-based application residing in the Treasury Web Application Infrastructure (TWA) located in Dallas. ECP serves as a link between all of the Revenue Collections Management (RCM) lockboxes, the Debit Gateway (DG), the Collections Information Repository (CIR), and the Image Archive. Federal government agencies and Treasury's lockbox financial agents use the ECP application to store and retrieve captured images and data of checks and remittance items, to facilitate paper check processing, and to provide detail and summary data of items processed at the RCM lockboxes to CIR. ECP currently supports approximately 1,200 users from 73 federal agencies and financial institutions, and in FY 2018, processed over 98 million transactions valued at more than \$458 billion. During April FY18 IRS peak period, ECP processed 22.1 million transactions totaling \$199.9 billion.

PROCESS FLOW



- 1) Incoming USPS and overnight Delivery or Mobile check Capture
- 2) Lockbox Financial Agent picks up mail and verifies items according to specification, completes data capture and scans checks and remittance images. Mobile app server aggregates data and creates ECP files. Lockbox FA and Mobile app server transmits payment/remittance data and images to ECP.
- 3) ECP deposit preparation, stores images and data, generates reports. Forwards financial items and images to the Debit Gateway, receives and updates data/statuses. Forwards settlement and return data to CIR.
- 4) Debit Gateway - Bank of First Deposit – Processes payments for settlement via Check 21 or ACH and sends settlement/return data back to ECP.
- 5) CIR – ECP Settlement and Return Data are available in voucher and financial transaction reporting.
- 6) Agencies may login to ECP to retrieve reports/images or login to GIR to view reports and deposit information.

III. OBJECTIVES

Fiscal Service is seeking one FA to achieve the following business objectives:

- Competition between Financial Institutions – By holding a competition for services, we expect to identify the most qualified FA that can provide the highest level of service at commercially reasonable prices.
- Improved Program Management – Fiscal Service expects to improve program management by partnering with an FA with extensive industry practice and technically skilled experienced employees with a track record of providing outstanding operational and customer service. The FA team should include a diverse mix of skill sets that correspond to major aspects of financial transaction processing, including IT development, operations, project management, analyses, security, and customer service. The FA team should also demonstrate the experience and ability to work cohesively with potential competitors to accomplish the Bureau of Fiscal Service’s operational and strategic goals.
- Industry and Technology Expertise – In this specialized business line, an FA with both technical and industry experience and certifications will best position ECP for success, security, stability, and redundancy. The FA will keep abreast of developments in financial transaction processing and offer best in class technical changes and innovative solutions. The FA will demonstrate a track record of reliability in meeting operational metrics and system availability
- Innovation and Process Improvement – Fiscal Service seeks an FA that can deliver innovation and process improvement to support major initiatives by increasing business agility and the number of software deployments. Some possible Bureau of Fiscal Service initiatives during the life of the agreement may include moving to a new environment and potentially integrating parts of ECP with other Fiscal Service applications.

IV. TECHNICAL AND PROCESSING REQUIREMENTS

A. ECP Core Processing Requirements

The FA will provide the following core processing requirements:

- **Daily Operations:** The FA will provide expert-level payment transaction processing and data reporting capabilities inclusive of balancing and reconciliation processes. The FA must have experience in daily operations to include file processing with partners, call center and customer service operations, systems operations and maintenance, security compliance, incident reporting, and the delivery of analytical products (comparative analysis, market research, information papers, identification of best practices, trends, patterns, compliance, etc.).

- **Operational Resiliency:** The FA must provide a high standard of operational resiliency for the ECP system that allows recovery and reconstitution of operations should unexpected outages or other interruptions occur. ECP application availability is 99% per month and the recovery time objective is 4 hours. The FA is expected to plan, test and demonstrate their readiness for the April IRS Peak period. In light of the cyber and overall threat to systems, the FA must maintain a high standard of resiliency strategies in terms of business continuity, disaster recovery and incident response. In addition, the FA should conduct routine failover exercises, playbooks, tabletop exercises and war games to continuously test and refine contingency processes and procedures.

- **Development:** The FA will be responsible for software development, patch releases, requirements gathering, documentation, and all forms of testing for the ECP system. The quality of code, testing, and technical problem resolution will require a qualified IT workforce with a mix of experience in web based applications, secure coding, interfaces that support direct file transmissions, Java development and technologies such as WebLogic, Oracle, Jasper, Connect Direct, and the Unix Sun Solaris platform.

- **Customer Service:** The FA will provide customer support for lockbox providers and Federal Agency users from Monday through Friday from 6:00 AM EST – 11:00 PM EST, as well as after hours on call, support as needed. The ECP user base consists of approximately 1,200 active users from 73 different agencies (392 active cashflows) and 8 lockbox providers. The FA must be able to answer inbound phone calls and respond to emails regarding various inquiries including, but not limited to; navigation assistance, technical support, reporting needs or discrepancies, account management, payment information and file transmissions. In addition, the FA needs to organize quarterly user and POC refresher training sessions, ad hoc training sessions as request by federal agencies and meet service level agreements that affect the customer experience and overall responsiveness to customers.

- **Program Management:** The FA must be committed to ECP system success through a dedicated operations staff with a mix of experience and skill sets to achieve effectiveness in all aspects of ECP system operations. The mix of skills includes but is not limited to:
 - Project management
 - Software development
 - Business and systems analysis
 - Business process improvement
 - Earned value management (EVM)
 - Incident management
 - Risk management
 - Statistics, forecasts and metrics reporting (trends/patterns)
 - Analysis
 - Compliance with service level agreements
 - Regulatory compliance
 - Internal controls
 - Reporting

- **Security and Compliance:** The FA must be committed to meeting Fiscal Service security standards and assurances, including personnel, physical and information technology standards.

B. Service Level Requirements

The FA will provide the highest standards of performance and quality, and must perform ongoing daily quality control reviews of work in process. Fiscal Service will review the established quality controls on an on-going basis to ensure performance meets established standards. This review will include accuracy, responsiveness, timeliness, system availability, and security.

C. Systems Interface

In addition to the RCM's Lockbox Services, the FA will be required to interface or work with partners of the following Fiscal Service systems:

1. Bank Management System (BMS)

BMS is the system used by Fiscal Service to review, approve, and pay expenses incurred by its Financial Agents. The FA will report its expenses each month through BMS.

2. Collections Information Repository (CIR)

CIR is a reporting system that consolidates detailed and summary-level information on collections transactions and reports this information to federal agencies and other Fiscal Service and Treasury systems. ECP sends settlement and return data to CIR for financial transaction reporting.

3. Debit Gateway (DG)

The DG is a Fiscal Service settlement mechanism used for the origination of ACH debit entries, and for converted and truncated check transactions. ECP sends files to the DG for settlement via Check 21 or ACH debit and sends settlement/return data back to ECP.

4. Treasury Web Application Infrastructure (TWAI)

The TWAI is the hosting platform for the ECP application, which is managed by the Federal Reserve Information Technology (FRIT) and Fiscal Service. The FA will be required to access TWAI resources related to the ECP application to support daily operations, and work with the TWAI to troubleshoot outages and deploy releases.

D. Security and Certification Requirements (Please see Attachment A for more information.)

- The FA will meet all applicable 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 Fiscal Service 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.
- The FA must ensure all employees and all contractors providing ECP services are citizens or lawful permanent residents of the United States. All facilities and systems used to provide ECP services must be located in the United States.
- The FA must adhere to all federal security requirements listed in Attachment A.

V. SUBMITTING PROPOSALS

A. Content

Proposals should clearly demonstrate the financial institution's ability to meet the requirements specified in Section IV. Proposals should also provide the following:

- Examples of major system implementations performed within the last three (3) years, with numbers of users, architecture, technologies used, and number of external interfaces;
- Experience with the following technologies and programming languages: WebLogic (Java EE), Oracle Database, Java, PL/SQL, CSS, UNIX shell scripting and Jasper on a UNIX Sun Solaris platform;
- Experience with Software Development Life Cycle (SDLC) techniques, in addition to Agile Development and other iterative software development methodologies;
- Experience integrating security through the SDLC and secure coding best practices;
- Identity and description of any proposed partners or contractors that will be providing ECP services;
- References, including private sector and government (other than U.S. Treasury), with appropriate contact information and project context;
- Recommendations for improving or replacing the ECP User Interface. Suggestions involving a commercial user interface are acceptable; and
- Any other relevant information to assist Fiscal Service in its evaluation of the respondent's proposal.

Proposal documents should not be marked as “*Proprietary and Confidential*”, and Fiscal Service 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.

B. Format Specifications:

Proposals must be formatted as follows:

- No more than 20, one-sided pages (not including any requested attachments)
- Paper size “8 ½ x 11”
- Single-spaced
- Font type and size – 12 point Times New Roman font
- Margin size – one inch
- A table of contents is optional (not included in 20-page maximum)
- Five paper copies of the proposal
- One CD containing (a) the proposal in Microsoft Word format and (b) a signed copy of the proposal in Adobe PDF format.

C. 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 Fiscal Service's FASP and is not subject to the Federal Acquisition Regulations.

D. Submission: Financial institutions should submit their proposals to Fiscal Service no later than 5:00 pm ET on June 5, 2019. Proposals should be sent by courier or traceable delivery service to:

**Mr. Michael Mackay
Director, Revenue & Remittance Management Division
U.S. Department of the Treasury
Bureau of Fiscal Service
401 14th Street, SW, Room 424
Washington, DC 20227**

E. Questions about the Solicitation: Financial institutions should direct all questions about this solicitation to the following mailbox address: ECPFASP@fiscal.treasury.gov. Fiscal Service 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.

VI. EVALUATION PROCESS

A. Phase 1

At the beginning of the evaluation process, each financial institution will be required to execute a non-disclosure agreement (Attachment B) before Fiscal Service will consider its proposal.

During Phase 1, Fiscal Service will evaluate proposals to determine the ability of the financial institution to meet the requirements specified in Sections IV, V and VI. Fiscal Service may conduct a Phase 1 information session for all applicants. The Phase 1 information session will provide information regarding the FASP, security, and interfaces with ECP, BMS, and other Fiscal Service systems. Applicants should RSVP for the initial Information Session to ECPFASP@fiscal.treasury.gov by May 15, 2019. A maximum of 3 representatives may attend from each FI. A completed non-disclosure agreement (NDA) will be required.

1. Scoring

Fiscal Service will evaluate all proposals received during Phase 1 and may, in its sole discretion, conclude the competition or select two financial institutions as finalists to move to Phase 2. Financial institutions not selected for Phase 2 will be notified.

B. Phase 2

Each finalist will be notified by Fiscal Service that its proposal warrants further consideration and will be invited to participate in Phase 2 of the evaluation process. Financial Institutions not selected as finalists will also be notified.

At the beginning of Phase 2, each finalist will receive a pricing template to submit their best and final transition and pricing proposals and a copy of the model FAA.

Fiscal Service will conduct a Phase 2 information session for all finalists. The Phase 2 session will provide detailed information regarding the pricing template, audit requirements, and Attachments A and B.

Additional information sessions consisting of open dialogue with Fiscal Service, both with individual finalists and collectively with all finalists, may occur at the discretion of Fiscal Service. Fiscal Service 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 proposal in an oral presentation held in person at Fiscal Service headquarters in Washington, D.C. After the oral presentations, Fiscal Service will select one finalist as the FA for the ECP. The FA will be required to execute the FAA with Fiscal Service in December 2019.

Evaluation Timeline

Fiscal Service plans to follow the schedule below, but dates may change at the sole discretion of Fiscal Service.

Timeline	Phases / Events
May 3, 2019	FASP Released
May 15, 2019	Initial Information Session RSVP Due
May 21, 2019	Initial Information Session and Non-Disclosure Form
June 5, 2019	Initial Proposals Due to Fiscal Service
TBD	Respondent FI Notification
TBD	Second Information Session
TBD	Final Proposal Due to Fiscal Service
TBD	Finalist presentations, including “Best and Final Offer” pricing
TBD	Selection, commencement of FAA negotiations
TBD	Signing of new FAA

C. Evaluation Criteria

Fiscal Service will evaluate proposals based on multiple factors. In Phase 1, Fiscal Service will consider only factors (a) - (f) set forth below. In Phase 2, Fiscal Service will consider all factors set forth below.

- a. Experience providing payment transaction processing and data reporting, including reconciliation, and providing customer service to a large customer base.
- b. Operational Resiliency – Ability to provide a standard of resiliency for the ECP system that allows for the recovery and resumption of operations should unexpected outages or other interruptions occur.
- c. Software Development - Ability to provide a qualified IT workforce with a mix of demonstrated experience in web-based applications, secure coding, testing automation tools, interfaces that support direct file transmissions, as well as experience with problem resolution. Commitment from the FA to work with Fiscal Service to integrate or transition parts of ECP to other Fiscal Service applications.
- d. Innovation and Process Improvement – Experience delivering innovative products and services to achieve process improvements, increase productivity and meet customer needs. Some examples of innovative products and services are Application

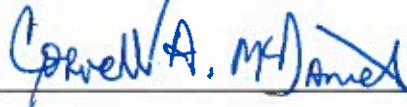
- d. Innovation and Process Improvement – Experience delivering innovative products and services to achieve process improvements, increase productivity and meet customer needs. Some examples of innovative products and services are Application Programming Interfaces (APIs), DevOps, Robotic Process Automation (RPA) and Testing Automation.
 - User Experience (UX) – The Financial Institution should demonstrate experience designing and delivering software enhancements focused on user-centric approaches while taking into account business goals and objectives.
- e. Program Management – Ability to provide an experienced dedicated operational staff with a mix of skill sets.
- f. Security and Compliance – Commitment to meeting Fiscal Service security standards and assurances, including personnel, physical and information technology. The FA is expected to have a dedicated resource to serve as the Information Security Officer (ISSO) for the ECP application.
- g. Transition Plan and Experience – Experience in knowledge transfer, setup of development and testing environments.
- h. Pricing proposal, including any costs for the transition to the financial institution.

VII. OTHER

This Financial Agent solicitation may be amended from time to time, or cancelled in its entirety, at the sole discretion of Fiscal Service.

VIII. ATTACHMENTS

- Attachment A—Security Requirements
- Attachment B—Non-disclosure Form
- Attachment C—Security Controls Rules of Behavior Agreement



Corvelli A. McDaniel
Assistant Commissioner, Revenue Collections Management

ATTACHMENT A

SECURITY REQUIREMENTS FOR FAA

1 Information Types

The term “information” is synonymous with data, regardless of format or medium. Personally Identifiable Information (PII) is a subset of Sensitive But Unclassified (SBU) information. Sensitive PII is a subset of PII, and therefore a subset of SBU information. All requirements for SBU information apply to PII and Sensitive PII. All requirements for PII apply to Sensitive PII.

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 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.

1.3 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 Fiscal Service procedures for proper handling of SBU 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.

Sensitive But Unclassified information, data, and/or equipment will only be disclosed to authorized personnel on a need-to-know basis. 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. Destruction of items shall be accomplished by following NIST Special Publication 800-88, Guidelines for Media Sanitization.

The disposition of all data will be at the written direction of Fiscal Service, 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 Fiscal Service.

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 and equipment

Information systems and services performing work on behalf of the Fiscal Service 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. Fiscal Service information shall be accessed only by personnel meeting or surpassing the Treasury citizenship requirements (as determined by Personnel Security, see section 7 below). Extra precautions should be in place for other types of access from foreign locations.

Work shall be performed on systems secured at least at a FIPS 199 MODERATE security category level.

Systems and services placed on the Fiscal Service portfolio must be authorized as per Fiscal Service SA&A and ISCM policies.

The financial agent must not remove SBU information from approved location(s), electronic device(s), or other container(s), without prior approval from the CIO or their designee.

Contracts and/or task orders for the acquisition of information systems or services processing SBU information for Fiscal Service shall require an acceptable Security Assessment & Authorization (SA&A)

or similar security assessment package as may be prescribed by Fiscal Service. The financial agent shall grant access to Fiscal Service to review any existing SA&A documentation.

When needed per Fiscal Service direction, the financial agent and Fiscal Service officials shall prepare an Interconnection Security Agreement (ISA) prior to connecting to external information systems and in accordance with Fiscal Service processes. Any computer equipment used by or on behalf of the Fiscal Service shall support Transport Layer Security (TLS) v 1.2 or greater and comply with current NIST guidance.

Cryptographic modules used to protect Fiscal Service information must be compliant with the current FIPS 140 version and validated by the Cryptographic Module Validation Program (CMVP). The financial agent must provide the validation certificate number to Fiscal Service for verification. Encryption is required to protect federal and financial agent data when transmitting between systems.

The financial agent shall be subject to periodic audits and reviews, as required by law. The financial agent shall provide reports with findings that result from audits and reviews to Fiscal Service.

The financial agent may be required to provide Fiscal Service access to, and information regarding systems the financial agent operates on behalf of Fiscal Service as part of its responsibility to ensure compliance with security requirements. Fiscal Service access may include independent validation testing of controls, system penetration testing, FISMA reviews, monthly data feed requirements as coordinated by Fiscal Service, and access by agency Inspector General for its review.

All information systems that input, store, process, and/or output Government information must be granted approval by the CIO, or designee for operation and/or use. The financial agent must adhere to current Fiscal Service policies, procedures, and guidance for Security Assessment and Authorization (SA&A) activities.

The financial agent shall allow for physical inspection of facilities by Fiscal Service or representatives at Fiscal Service's discretion, including in the event of a computer security incident. The agreement shall specify access rights to financial agent facilities as appropriate. A computer security incident is defined as any adverse event that threatens computer security and may include but is not limited to: loss of data confidentiality, disruption to data or system integrity, and denial of availability.

The financial agent shall report any suspected security incident by phone to the Fiscal Service IT Service Desk within one hour of identification of a suspected security incident: 304-480-7777.

3 Federal Regulatory Requirements and Industry Standards

The financial agent's performance and systems shall comply with applicable federal government laws, directives, executive orders, standards, guidelines, and other requirements for information security, personnel security, physical security, and data encryption. The financial agent's performance and systems shall comply with the most current versions of the following applicable Federal and industry information technology regulatory requirements and standards:

- Federal Information Security Modernization Act of 2014 (FISMA)
- FIPS 140-2, 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
- FIPS 201-2, Personal Identity Verification for Federal Employees and Contractors
- Fiscal Service Baseline Security Requirements (BLSRs)
- NIST SP 800-30, Guide to Conducting Risk Assessments
- NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations
- NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations
- NIST SP 800-63-3, Electronic Authentication Guideline
- NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations
- OMB Circular A-130, Management of Federal Information Resources
- OMB M-04-04, E-Authentication Guidance for Federal Agencies
- OMB M-14-03, Enhancing the Security of Federal Information and Information Systems
- OMB M-07-16, Safeguarding Against and Responding to the Breach of PII 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

New regulatory requirements and standards shall be adhered to as they are enacted or become effective, as applicable. The financial agent shall implement a process to support timely compliance with new requirements imposed by external authorities.

The financial agent shall comply with both Fiscal Service and Treasury requirements that extend above federal government and industry information technology regulatory requirements and standards.

3.1 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 Fiscal Service or to accomplish a Fiscal Service function for a System of Records (SOR)¹. Financial agents must assist in the completion of any required Privacy Threshold Analysis (PTA) and/or Privacy Impact Analysis (PIA).
- (b) In the event of violations of the Act, a civil action may be brought against Fiscal Service when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an Fiscal Service function, and criminal penalties may be imposed upon the officers or employees of Fiscal Service when the violation concerns the operation of a SOR on individuals to accomplish an Fiscal Service function. For purposes of the Act, when the agreement is for the operation of a SOR on individuals to accomplish a Fiscal Service function, the financial agent is considered to be an employee of the agency.

4 Security and Privacy Awareness Training

The financial agent personnel who require access to Fiscal Service information or information systems will be required to review and sign Rules of Behavior, and complete security awareness training prior to being granted access. For the first 60 days of user access, reviewing and signing the Rules of Behavior is adequate for meeting the security awareness training requirement. If the security awareness training requirement is not completed, access may be revoked. Security and Privacy training will be required on a recurring annual basis, of all financial agent staff performing work for Fiscal Service, provided by Fiscal Service 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.

5 Bureau of the Fiscal Service (Fiscal Service) Personnel Security Requirements

The Bureau of the Fiscal Service (Fiscal Service) has determined that performance of this agreement requires that the financial agent, and vendor(s) (herein known as Contractor), requires access to Sensitive but Unclassified (SBU) information (herein known as unclassified information) and evaluated as:

"Moderate Risk" - All financial agent who require access to Treasury or Bureau-owned or controlled facilities and security items or products, shall either be United States Citizens or have lawful Permanent Resident Alien status, with at least three (3) or more years of United States residency.

The financial agent will abide by the requirements set forth in the Non-Disclosure Agreement, included in the FAA, for the protection of unclassified information at its cleared facility. If the financial agent has

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.

access to unclassified information at the Fiscal Service or other Government Facility, it will abide by the requirements set by that agency.

6 Proposal Instructions

6.1 READING ROOM FOR SECURITY CONTROL REVIEW

Prior to proposal submission, the financial institution may schedule an appointment to review documentation for the security control requirements. Due to the security sensitive nature of this documentation, the Fiscal Service will not release this information as part of a Request for Proposals or other equivalent document. Appointments will be made for review of security control requirements documentation. Appointments will be scheduled for two hour blocks based on Fiscal Service's representative's availability. Documentation reviews will be conducted Washington, D.C. area (Hyattsville office) in Treasury offices.

The financial institution shall be permitted to send a maximum of three staff to review documentation. The financial institution's staff performing documentation review shall be U.S. Citizens. The financial institution shall provide the Fiscal Service with the full name, for each staff member the financial institution plans to send to review documentation. A signed Fiscal Service Security Controls Rules of Behavior Agreement, Attachment C, and a signed Non-disclosure Agreement, Attachment B, is required prior to the review. This information shall be provided to PRMB.IAD-ISS@fiscal.treasury.gov prior to 1:00 PM Eastern Time at least five (5) Government business days prior to scheduled appointment.

The financial institution's staff members who have not supplied the requested information will not be permitted to review security control requirements documentation. The financial institution's staff shall present a photo ID issued by a federal or state government organization when they arrive to review documentation. The name on the photo ID must match the name previously provided to Fiscal Service. The financial institution staff will be escorted and will not be permitted to remove copies of any documentation.

The financial institution shall provide Fiscal Service with the full name, for each staff member, or others whom the financial institution intends to grant access to information about security control requirements; the financial institution shall provide this information to Fiscal Service at least five (5) Government business days prior to scheduled reading room access appointment. All persons provided access to information about security control requirements by financial institution shall be US citizens. The financial institution shall not permit any individuals of whom Fiscal Service does not approve to have access to security control requirements information.

If the financial institution intends to send staff with portable electronic devices (PEDs), the financial institution shall provide Fiscal Service with the name of the encryption software product and the version number of the software at the time appointments are scheduled -- before 4:00 PM Eastern Time at least five (5) Government business days prior to scheduled reading room access appointment. Fiscal Service will not permit notes about security control requirements to be made using any unencrypted PED. Fiscal Service will confirm FIPS 140-2 validation and inspect PEDs. Should a financial institution arrive with a

PED that does not have FIPS 140-2 validated full disk encryption software in use, the Fiscal Service will not permit the PED to be used.

6.2 Additional Instructions

The financial institution shall explain in proposal how the financial institution plans to secure Fiscal Service information in accordance with the requirements of this solicitation.

The financial institution is responsible for the proper handling and protection of Sensitive Information to prevent unauthorized disclosure. The financial institution must produce policy documentation

The financial institution shall explain in proposal their process to support timely compliance with new security requirements and standards imposed by external authorities.

Demonstrations

Financial institution demonstrations shall not be conducted using systems containing SBU, PII, or other sensitive information.

ATTACHMENT B

NON-DISCLOSURE AGREEMENT

Between

U.S. Department of the Treasury, Bureau of the Fiscal Service,
and

[Bank's Registered Name]

WHEREAS, the U.S. Department of the Treasury, Bureau of the Fiscal Service ("Fiscal Service") is currently soliciting proposals from commercial banks for the Electronic Check Processing (ECP), as well as the day-to-day operations of the ECP Program;

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

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

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

- 1) **Confidential Information.** Fiscal Service may, in its sole discretion, disclose to Bank the following documents and information about the Fiscal Service ECP applications, which constitute Confidential Information: source code, data or methods, documentation such as use cases, screen prints, details of interfaces, application architecture, security, operating procedures, authentication and authorization approaches for ECP, information about Treasury Systems Interfaces of the Collection Information Repository (CIR), Debit Gateway and Bank Management System (BMS) and any other Sensitive But Unclassified ("SBU") or Confidential.
- 2) **No Representation as to Future Work.** Bank expressly acknowledges that it may not be selected as the financial agent pursuant to the ECP FASP, and that any costs or expenses incurred by it in preparing a proposals 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 ECP 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 proposals in connection with the ECP 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 proposals for the ECP 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.** Fiscal Service 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 Fiscal Service 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 Fiscal Service, and that money damages would not be a sufficient remedy for breach of the confidentiality obligations of this Agreement. Accordingly, Fiscal Service 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 Fiscal Service within five working days of notice of non-selection in the event that Bank is not selected to perform any work pursuant to the ECP 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 Fiscal Service, 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.”
- 14) **Disclosure** Notwithstanding anything to the contrary contained herein, the Bank and its affiliates may disclose Confidential Information, after providing notice to Fiscal Service, to any governmental agency or regulatory authority having authority to regulate or oversee any aspect of the Bank’s business or that of its affiliates in connection with the exercise of such authority.

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.

Michael Mackay
 Director, Revenue and Remittance Management Division
 Bureau of the Fiscal Service
 U.S. Department of the Treasury

 Date

 [NAME]
 [TITLE]
 [Bank’s Registered Name]

 Date

Its: _____

ATTACHMENT C

SECURITY CONTROLS RULES OF BEHAVIOR AGREEMENT

I, _____, hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain United States Government documents or material containing sensitive but unclassified information. I understand and agree to the following terms and conditions:

Upon signing this Security Controls Rules of Behavior and a Non-Disclosure Agreement, I will be permitted access to official Bureau of the Fiscal Service documents containing sensitive but unclassified information related to security controls and understand that no copies may be made from the originals. Any notes I take during the course of such access shall be provided to Fiscal Service for review prior to my departure. I shall not allow any individuals access to security control requirements information without Fiscal Service's approval and the individual's signed 'Security Controls Rules of Behavior' (this information includes notes Fiscal Service permits to leave the controlled Reading Room appointment area along with notes and working papers created after the review appointment)

If I take any notes during the security control requirement documentation review using a portable electronic device (PED), such as but not limited to a laptop computer, the PED shall have FIPS 140-2 validated full disk encryption in use.

At no time will I transmit, transport, process, or store information about security control requirements in any location located outside of the United States.

I will return all paper copies of any notes about the security control requirements, including notes and working papers created after the security control requirement documentation review appointment, to Fiscal Service with my proposal or when I determine a proposal will not be submitted. I will destroy all electronic copies of any notes relating to security control requirements in accordance with NIST SP 800-12 and NIST SP 800-88. I will include in my proposal a notice to the Fiscal Service attesting to such file destruction; should I not make a proposal, I will send notice to the Fiscal Service attesting to the destruction of the files.

I make this Agreement in good faith, without mental reservation or purpose of evasion.

Printed Name

Signature

Date