



REQUEST FOR PROPOSALS FOR

**Marketing Automation System for the
Pennsylvania Treasury Department**

ISSUING OFFICE

**Pennsylvania Treasury Department
Bureau of Support Services
Procurement Division
Room 3T, Finance Building
Harrisburg, PA 17120-0018**

RFP 18-002

DATE OF ISSUANCE

February 4, 2019



REQUEST FOR PROPOSALS FOR
Marketing Automation System for the
Pennsylvania Treasury Department

TABLE OF CONTENTS

CALENDAR OF EVENTS	iii
Part I—GENERAL INFORMATION	1
Part II—PROPOSAL REQUIREMENTS	10
Part III—CRITERIA FOR SELECTION	13
Part IV—WORK STATEMENT/REQUIREMENTS	15
LIST OF ATTACHMENTS & APPENDICES	20



CALENDAR OF EVENTS

Treasury will make every effort to adhere to the following schedule:

Activity	Responsibility	Date
RFP Issued and Posted to www.patreasury.gov	Issuing Office	February 4, 2019
Deadline for Written Question Submission	Vendors	February 15, 2019
Answers to Written Questions Distributed	Issuing Office	February 25, 2019
Vendor Presentations	Issuing Office	Week of March 25, 2019
Sealed Proposals Received No Later Than 4:00 P.M. at: Pennsylvania Treasury Department Bureau of Support Services Procurement Division Room 3T, Finance Building Harrisburg, PA 17120 Attention: Mark Lavelle	Vendors	March, 11, 2019

Treasury has the right to change the above dates and times, and if so, each Vendor shall be responsible for monitoring the Treasury website (www.patreasury.gov) for new or revised RFP information.

PART I

GENERAL INFORMATION

I-1. Purpose

This Request for Proposals (“RFP”) provides to those interested in submitting proposals for the subject procurement (“Vendors”) sufficient information to enable them to prepare and submit proposals for the Pennsylvania Treasury Department (“Treasury” or “Department”) to provide a Marketing Automation System (“System”) for use throughout the Department. Unless otherwise stated, herein “Commonwealth” shall refer to all other state agencies, Boards or Commissions.

Treasury requires a System that will a) streamline how it gathers data and stores contacts and client information, b) reduce the work required to issue marketing communications, and c) interface with Treasury users’ existing recordkeeping platforms in order to accomplish these requirements. Such a System will allow Treasury to communicate more effectively with our customers, our stakeholders, and the citizens of Pennsylvania. While Treasury prefers a System that is housed at and maintained by the Vendor, it will accept proposals that offer a solution that envisions the System being housed at and maintained by Treasury.

Treasury now seeks proposals to provide products and/or services necessary to implement, customize, and support a System (“Products and Services”) as further described in Part IV Work Statement/Requirements.

I-2. Scope

This RFP seeks information to demonstrate the Vendor's ability to provide specific functions in terms of service, performance, capacity, and capability. This RFP contains instructions governing the requested proposals, including the requirements for the information and material to be included; a description of the services to be provided; requirements which Vendors must meet to be eligible for consideration; general evaluation criteria; and other requirements specific to this RFP.

I-3. Issuing Office

Treasury is the “Issuing Office.” The sole point of contact for this RFP shall be Mark Lavelle, Chief Administrative Officer (“Issuing Officer”). Any inquiries relating to your submission should be sent to the Issuing Officer by email at RFP18-002@patreasury.gov.

I-4. Problem Statement

Absence of a Marketing Automation System. Treasury is seeking proposals to provide Products and Services necessary to provide a System including necessary customization, implementation, and ongoing support.

I-5. Questions and Answers

Vendors must submit questions by email (with the subject line **RFP 18-002 Questions**) to the Issuing Officer, Mark Lavelle at RFP18-002@patreasury.gov. The Vendor shall not attempt to contact the

Issuing Officer by any other means. The Issuing Officer shall transmit all questions and responses to each Vendor that has received this RFP.

Each Vendor shall be responsible for monitoring the Treasury website for new or revised RFP information. The Issuing Office shall not be bound by any verbal information nor shall it be bound by any written information that is not either contained within the RFP or formally issued as an addendum by the Issuing Office. The Issuing Office does not consider questions to be a protest of the specifications or of the solicitation.

I-6. Pre-proposal Conference

There will be no pre-proposal conference.

I-7. Contracting Terms and Conditions

In the event that the Issuing Office enters into a contract as a result of this RFP, it is the intention to utilize a contract containing the Standard Contract Terms and Conditions as shown in Appendix F.

The Issuing Office, in its sole discretion, may undertake negotiations with Vendors whose proposals, in the judgment of the Issuing Office, show them to be qualified, responsible, and capable of performing the services described in this RFP.

I-8. Electronic Version of RFP

This RFP is being made available via the Treasury website (www.patreaury.gov). The Vendor acknowledges and accepts full responsibility to ensure that its proposal responds to the RFP as published on this website, as amended, if at all, by subsequent electronic means and/or addenda on the Treasury website. In the event of a conflict between a version of the RFP in the Vendor's possession and the Issuing Office's final version of the RFP, the Issuing Office's final version shall govern.

I-9. Addenda to RFP

If the Issuing Office deems it necessary to revise any part of this RFP before the proposal response date, it will publish updated documents on the Treasury website (www.patreaury.gov). Notice also will be provided to the entities through which this RFP is distributed.

I-10. Response Date

To be considered, each Vendor must submit eight hard copies of its proposal to the Issuing Office on or before the time and date specified in the Calendar of Events on page iii of this RFP. Additionally, each Vendor shall email an electronic copy of its proposal to the Issuing Officer, Mark Lavelle, at RFP18-002@patreaury.gov on or before the time and date specified in the Calendar of Events on page iii of this RFP. Late proposals shall not be considered.

Please remember to allow sufficient mail delivery time to ensure timely receipt of the proposal. If, due to inclement weather, natural disaster, or any other cause, the Issuing Office location to which proposals are to be returned is closed on the proposal response date, the deadline for submission shall be automatically extended until the next business day on which the Issuing Office is open, unless the Vendors are otherwise notified by Treasury. The time for submission of proposals shall remain the same even if the response date is extended. Late proposals shall not be considered.

I-11. Incurring Costs

The Issuing Office is not liable for any costs the Vendor incurs in preparation and submission of its proposal, in participating in the RFP process, or in anticipation of award of the contract.

I-12. Economy of Preparation

Vendors should submit proposals that are simple and provide a straightforward, concise description of the Vendor's ability to meet the requirements of the RFP.

I-13. Proposal Contents

- a. **Confidential Information.** Treasury is not requesting, and does not require, confidential proprietary information or trade secrets to be included as part of Vendors' submissions in order to evaluate proposals submitted in response to this RFP. Accordingly, except as provided herein, Vendors should not label proposal submissions as confidential or proprietary or trade secret protected. Any Vendor that determines that it must divulge such information as part of its proposal must follow the procedure described below:
 - (1) Prepare an un-redacted version of the appropriate document, and
 - (2) Prepare a redacted version of the document that redacts the information that is asserted to be confidential or proprietary information or a trade secret, and
 - (3) Prepare a signed written statement that states:
 - i) The attached document contains confidential or proprietary information or trade secrets;
 - ii) The Vendor is submitting the document in both redacted and un-redacted format in accordance with 65 P.S. § 67.707(b); and
 - iii) The Vendor is requesting that the document be considered exempt under 65 P.S. § 67.708(b)(11) from public records requests.
 - (4) Submit the documents along with the signed written statement to Treasury.
 - (5) This information may be subject to Right-to-Know Law.
- b. **Treasury Use.** All material submitted with the proposal shall be considered the property of Treasury and may be returned only at the Issuing Office's option. Treasury has the right to use any or all ideas not protected by intellectual property rights that are presented in any proposal regardless of whether the proposal becomes part of a contract. Notwithstanding any Vendor copyright designations contained on proposals, Treasury shall have the right to make copies and distribute proposals internally and to comply with public record or other disclosure requirements under the provisions of any Commonwealth or United States statute or regulation, or rule or order of any court of competent jurisdiction.
- c. **Public Disclosure.** After the award of a contract pursuant to this RFP, all proposal submissions are subject to disclosure in response to a request for public records made under the

Pennsylvania Right-to-Know-Law, 65 P.S. § 67.101, et seq. If a proposal submission contains confidential proprietary information or trade secrets, a signed written statement to this effect must be provided with the submission in accordance with 65 P.S. § 67.707(b) for the information to be considered exempt under 65 P.S. § 67.708(b)(11) from public records requests. Financial capability information submitted in response to this RFP is exempt from public records disclosure under 65 P.S. § 67.708(b)(26).

I-14. Vendor's Representations and Authorizations

By submitting its proposal, each Vendor understands, represents, and acknowledges that:

- a. All of the Vendor's information and representations in the proposal are material and important, and the Issuing Office may rely upon the contents of the proposal in making an award. Treasury shall treat any misstatement, omission or misrepresentation as fraudulent concealment of the true facts relating to the proposal submission, punishable pursuant to 18 Pa. C.S. § 4904.
- b. The Vendor has arrived at the price(s) and amounts in its proposal independently and without consultation, communication, or agreement with any other Vendor or potential Vendor. This provision has no application to those Vendors who partner to provide a comprehensive solution.
- c. The Vendor has not disclosed the price(s), the amount of the proposal, nor the approximate price(s) or amount(s) of its proposal to any other firm or person who is a Vendor or potential Vendor for this RFP, and the Vendor shall not disclose any of these items on or before the proposal submission deadline specified in the Calendar of Events of this RFP.
- d. The Vendor has not attempted, nor will it attempt, to induce any firm or person to refrain from submitting a proposal on this contract, or to submit a proposal higher than this proposal, or to submit any intentionally high or noncompetitive proposal or other form of complementary proposal.
- e. The Vendor makes its proposal in good faith and not pursuant to any agreement or discussion with, or inducement from, any firm or person to submit a complementary or other noncompetitive proposal.
- f. To the best knowledge of the person signing the proposal for the Vendor, the Vendor, its affiliates, subsidiaries, officers, directors, and employees are not currently under investigation by any governmental agency and have not in the last **four** years been convicted or found liable for any act prohibited by State or Federal law in any jurisdiction, involving conspiracy or collusion with respect to bidding or proposing on any public contract, except as the Vendor has disclosed in its proposal.
- g. To the best of the knowledge of the person signing the proposal for the Vendor and except as the Vendor has otherwise disclosed in its proposal, the Vendor has no outstanding, delinquent obligations to the Commonwealth including, but not limited to, any state tax liability not being contested on appeal or other obligation of the Vendor that is owed to the Commonwealth.
- h. The Vendor is not currently under suspension or debarment by the Commonwealth, any other state or the federal government, and if the Vendor cannot so certify, then it shall submit along with its proposal a written explanation of why it cannot make such certification.

- i. The Vendor has not made, under separate contract with the Issuing Office, any recommendations to the Issuing Office concerning the need for the solution described in its proposal.
- j. Each Vendor, by submitting its proposal, authorizes Commonwealth agencies to release to the Issuing Office information concerning the Vendor's Pennsylvania taxes, unemployment compensation and workers' compensation liabilities.
- k. Until the selected Vendor receives a fully executed contract from the Issuing Office, there is no legal and valid contract, in law or in equity, and the Vendor shall not begin to perform.

I-15. Restriction of Contact

From the issue date of this RFP until the Issuing Office selects a proposal for award, the Issuing Officer is the sole point of contact concerning this RFP. Any violation of this condition may be cause for the Issuing Office to reject the offending Vendor's proposal. If the Issuing Office later discovers that the Vendor has engaged in any violations of this condition, the Issuing Office may reject the offending Vendor's proposal or rescind its contract award pursuant to terms and conditions.

Vendors must agree not to distribute any part of their proposals beyond the Issuing Office. A Vendor who shares information contained in its proposal with other Treasury personnel and/or competing Vendor personnel may be disqualified.

I-16. Prime Vendor Responsibilities

The selected Vendor will be required to assume responsibility for all services offered in the proposal whether it produces them itself or by subcontract. The Issuing Office will consider the selected Vendor to be the sole point of contact with regard to contractual and contract matters. Any function that will be subcontracted must be identified in the proposal. Treasury reserves the right to approve or reject any subcontractor. The selection of any subcontractor must be approved in writing by Treasury.

I-17. Rejection of Proposals

The Issuing Office reserves the right, in its sole and complete discretion, to reject any or all proposals received in response to this RFP.

I-18. Discussion for Clarifications

Vendors may be required to make an oral or written clarification of their proposals to the Issuing Office to ensure thorough mutual understanding and Vendor responsiveness to the solicitation requirements. The Issuing Office will initiate requests for clarification.

I-19. Best and Final Offer

While not required, the Issuing Office reserves the right to conduct discussions with Vendors for the purpose of obtaining "best and final offers." To obtain best and final offers from Vendors, the Issuing Office may do one or more of the following:

- a. Schedule individual interviews;
- b. Request revised proposals;
- c. Enter into pre-selection negotiations.

The Issuing Office will limit any discussions to responsible Vendors (those that have submitted responsive proposals and possess the capability to fully perform the contract requirements in all respects and the integrity and reliability to assure good faith performance) whose proposals the Issuing Office has determined to be reasonably susceptible of being selected for award. The requirements listed in Part II shall also be used to evaluate the best and final offers.

I-20. Notification of Selection

The Issuing Office will notify the selected Vendor in writing of its selection for negotiation after the Issuing Office has determined, taking into consideration all of the evaluation factors, the proposal that is the most advantageous to Treasury.

I-21. Term of Contract

The term of the Contract will commence on the Effective Date and will extend for **five (5) years, with the option to renew for one (1) additional two-year period. The Contract must grant to Treasury sole discretion to determine the exercise of renewal options, if any, in single or multiple year increments.** The Issuing Office will fix the Effective Date after the Contract has been fully executed by the selected Vendor and by Treasury and all approvals required by Commonwealth contracting procedures have been obtained. The Contract shall include a provision, typical in Commonwealth contracts, permitting at-will termination by the Commonwealth, upon adequate notice. Treasury will work with the selected Vendor to consider provisions to mitigate the risk of such termination.

Negotiations for any or all of the Products and Services may be undertaken with Vendors whose proposals show them to be qualified, responsible and capable of performing the work; whose proposals provide the Commonwealth with services that best meet the needs of the Commonwealth; and whose bids are favorable relative to other proposals.

If the Department determines that doing so is in its best interests Treasury may accept or reject any or all proposals; it may also accept or reject portions of proposals deemed to be severable by the appropriate Vendor and Treasury.

I-22. New Releases

Vendors shall not issue news releases, internet postings, advertisements or any other public communications pertaining to this project without prior written approval of the Issuing Office, and then only in coordination with the Issuing Office.

I-23. Presentations

Vendors will be required to make demonstrations of the Products and Services that they propose to provide to review their capabilities and qualifications to perform as described in their written response to the RFP. Such demonstrations provide an opportunity for the Vendors to clarify their proposals, thus ensuring a thorough mutual understanding of the Products and Services to be provided to Treasury. Treasury will schedule presentations as applicable.

I-24. Indemnification

For all Services contemplated under the terms of this RFP, Treasury will require the successful Vendor, and its subcontractors, to agree to the following contractual language: Vendor hereby indemnifies and agrees to defend, hold and save harmless the Commonwealth of Pennsylvania, the State Treasurer, Treasury and its employees, and the Tuition Account Programs Advisory Board from any and all claims, suits, actions, liabilities, and costs of any kind whatsoever resulting from Vendor's negligence or intentional misconduct in the administration of any contract that results from this RFP.

I-25. Insurance Requirements

A. Professional Liability Insurance.

A Certificate of Insurance demonstrating Professional Liability Insurance coverage in a minimum amount of one million dollars (\$1,000,000) is required to be submitted upon signing any contract that may be executed as a result of this RFP. The Professional Liability policy should have defense coverage provided in addition to this limit; if this is not feasible or possible, the limit of ten million dollars (\$10,000,000) is to be evidenced. Any deductible or self-insured retention shall be borne by the Vendor. This coverage must be maintained for at least five years beyond the termination of the contract. Insurance carrier must have an AM Best's rating of "A-" or better unless otherwise approved by Treasury.

B. Errors and Omissions Insurance Policy

An Errors and Omissions Insurance Policy with a limit of liability in the amount of a minimum of \$1,000,000 to cover the vendor and their respective officers, employees, agents and affiliates. Certification of such insurance policy is required to be submitted upon signing any contract that may be executed as a result of this RFP.

C. General Liability Insurance.

A General Liability policy in the amount of ten million dollars (\$10,000,000) is to contain, or be endorsed to contain, the following provisions:

1. The Commonwealth of Pennsylvania, the State Treasurer, Treasury and its employees, and the Pennsylvania Tuition Account Programs Advisory Board are to be covered as Additional Insureds.
2. For any claims related to the services performed pursuant to any contract that may be executed as a result of this RFP, the insurance coverage shall be primary insurance as respects the Commonwealth of Pennsylvania, the State Treasurer, Treasury and its employees, and the Pennsylvania Tuition Account Programs Advisory Board. Any insurance or self-insurance maintained by the Commonwealth of Pennsylvania, the State Treasurer, Treasury and its employees, and the Pennsylvania Tuition Account Programs Advisory Board shall be secondary to the Vendor's insurance.
3. The General Liability policy shall be endorsed to state that coverage shall not be canceled by the Insurer except after thirty (30) days prior written notice has been given to Treasury.

4. If General Liability, and/or Errors & Omissions (Professional Liability) coverage is written on a Claims Made form, the “Retro Date” must be shown, and must be before the date of any contract or the beginning of contract work.
5. Insurance must be maintained and evidence of insurance must be provided for at least five (5) years after completion of any contract work. Insurance carrier must have an AM Best's rating of “A-” or better.

D. Cyber Liability Insurance.

In the event that data will be housed and maintained at the Vendor’s location, upon signing any contract that may be executed as a result of this RFP, the Vendor shall secure and maintain during the term of the Contract data privacy and network security or cyber liability insurance, with a limit of not less than five million dollars (\$5,000,000).

I-26. Transition Upon Termination

Upon termination of any Contract that may be executed as a result of this RFP, the selected Vendor will be required, at no additional cost to the Department, to assist in the transfer of responsibilities, including but not limited to records and investment assets, to the Department or a successor Vendor.

PART II

PROPOSAL REQUIREMENTS

II-1. Format for Required Information. All proposals must be submitted using the following format. There must be four (4) distinct parts and a separate, sealed cost proposal, as presented in Parts II-2 to II-6 below. Each of these Parts must be completely addressed and responded to in the RFP, otherwise the proposal will be deemed incomplete and not eligible for consideration. Any supplemental information thought to be relevant, but not applicable to the enumerated categories, should be provided as an Exhibit to the proposal.

II-2. Tab 1: Vendor’s Understanding of Needs.

- A. State in succinct terms your understanding of the Products and Services required by this RFP.
- B. Do you expect to be able to implement a System within 60 days of execution of a contract with Treasury? If not, then what is the soonest you would anticipate being able to offer implement a System?
- C. What are the three biggest obstacles to being able to implement a System within 60 days?
- D. How do you propose to create interfaces with the users existing recordkeeping platforms?
- E. While it is Treasury’s preference that the Vendor store Treasury data, proposals that envision data storage at Treasury will be accepted. Do you propose to store Treasury data or do you expect Treasury to do this?
- F. If Treasury data will be stored by you, please provide a detailed description of the measures that you take to ensure the security of the data stored in your systems and the steps that are taken in the event of a breach. See Appendix F for more information.

II-3. Tab 2: Mandatory Minimum Qualifications.

- A. The Vendor must meet all of the following minimum qualifications, and agree to meet each of the following requirements, to be given further consideration. Failure to satisfy each of the minimum qualifications, or agree to meet each of the following requirements, will result in the immediate rejection of the proposal.
 - 1. The Products and Services must allow the import and use of external lists of contact information, including, but not limited to, names, home and mobile telephone numbers, mailing addresses, and email addresses.
 - 2. The Products and Services must allow for unlimited contacts (email, direct mail, SMS messaging, etc.) without the need for additional modules or purchases.
 - 3. A demonstration of the Products and Services must be held at Treasury and any expense incurred in conducting this demonstration, including, but not limited to, travel, lodgings, and meals, will be the sole responsibility of the Vendor.

4. The demonstration explained in Section II-3.A.3. must be conducted between March 25, 2019 and March 29, 2019.
5. In the event that data will be housed and maintained at the Vendor's location, the Vendor must agree to and be bound by the stipulations found in the Hosted Services Response Acceptability Stipulations found in Appendix F.

II-3. Tab 3: Work Plan. Describe your technical plan to demonstrate that you are able to implement the Products and Services required by this RFP. Organize your proposal according to Section IV-2, Products and Services to be Provided, restating each question before providing your answer.

II-4. Tab 4: Prior Experience.

A. Characteristics of Firm

1. State the name, address, telephone, e-mail address and fax number of the principal contact from the firm for this response.
2. Identify the entity that will execute the contract, as well as all affiliates, subsidiaries, subcontractors and other entities that will provide services to meet the requirements of this engagement.
3. If the party that will execute the contract is not a parent entity, indicate your willingness to provide a parent guarantee or propose a suitable alternative (e.g., letter of credit, insurance coverage, surety bond) to ensure performance of the services to be provided.
4. Provide a summary of the firm, including year formed, history, ownership structure, names of owners or partners, subsidiary or affiliate relationships, and the reporting and control structure. Do senior executives have ownership interests in the firm?
5. Please provide audited financial statements for the past three (3) fiscal years (include as an Exhibit to your response).
6. Has your firm experienced a data breach in the last five (5) years?
7. What is the firm's breach notification policy? Does it comply with the stipulations in Appendix F?
8. Please describe minimum performance standards under which your firm operates for areas such as system downtime and technical assistance. Please see the model service level agreement metrics in Appendix F.

B. Other Clients

1. List complete the following table with three current clients as references. To the extent possible, these references should be for clients for which the firm provides similar products and services. For “Contact Information”, please provide an email and a phone number; and for the “Specific Products/Services Provided”, please the nature of the products and services and their similarity to the Products and Services required by this RFP.

Client Name Contact and Title	Contact Information	Specific Products/Services Provided

II - 5. Tab 5: Personnel

- A. Please provide an organizational chart showing the project team members and the roles each will play in this engagement. Please indicate clearly who will serve as project manager.
- B. Please provide a resume for each individual included in your response to the immediately preceding question.
- C. If subcontractors are to be used, please provide identical personnel information for each subcontractor.

II-6. Cost Submittal

The Cost Submittal shall be provided in a separate electronic document. In completing the Cost Submittal, Vendors shall use the RFP 18-002 Cost Response included in Attachment B of this RFP.

The Cost Submittal shall be placed in a separate sealed envelope clearly labeled Cost Submittal and separated from the information included in Tabs 1 through 5 above.

The Vendor shall agree that all terms, warranties, and prices, as a whole, are comparable to or better than the equivalent terms, warranties, and prices, as a whole, offered by the Vendor to any present customer meeting substantially the same requirements or qualifications as Treasury. If the Vendor shall, during the term of this contract, enter into arrangements with any other customer providing greater benefits or more favorable terms, as a whole, the Vendor shall provide the same to Treasury.

The Cost Proposal must not include exceptions or additional terms and conditions.

Vendors should direct in writing to the Issuing Office pursuant to Part I, Section I-5, of this RFP any questions about whether a cost or other component is included or applies. All Vendors will then have the benefit of the Issuing Office’s written answer so that all proposals are submitted on the same basis.

PART III
CRITERIA FOR SELECTION

III-1. Proposal Evaluation

The Treasurer, or his designee, will appoint an RFP Evaluation Committee (hereinafter the "Committee") to review the proposals. The Committee will begin review of proposals as soon as practical after receipt. The Committee will be responsible for reviewing and evaluating all proposals for an understanding of the Products and Services required, qualifications of the Vendor, qualifications of personnel, soundness of approach and fees. The Committee will recommend for selection the proposal which it determines is the most advantageous to Treasury after considering all the evaluation factors.

Treasury may conduct negotiations with responsible Vendors. Award will only be made to a Vendor determined to be responsible in accordance with Commonwealth Management Directive 215.9, Contractor Responsibility Provisions, which are included in Appendix C. If Treasury determines that doing so is in the best interests of the PA 529, it may accept or reject any or all proposals; it may also accept or reject portions of proposals deemed to be severable by the appropriate Vendor.

III-2. Mandatory Responsiveness Requirements

To be eligible for selection, a proposal must be:

- A. Timely received from the Vendor; and
- B. Properly signed by the Vendor.

III-3. Nonconforming Proposals

The Issuing Office reserves the right, in its sole discretion, to waive technical or immaterial nonconformities in a Vendor's proposal.

III-4. Vendor Responsibility

To be responsible, a Vendor must submit a responsive proposal and possess the capability to fully perform the Contract requirements and the integrity and reliability to assure good faith performance of the contract.

In order for a Vendor to be considered responsible for this RFP, the Vendor's financial information must demonstrate that the Vendor possesses the financial capability to assure good faith performance of the contract. The Issuing Office will review the Vendor's previous three financial statements, any additional information received from the Vendor, and any other publicly-available financial information concerning the Vendor, and assess each Vendor's financial capacity based on calculating and analyzing various financial ratios.

A Vendor which fails to demonstrate sufficient financial capability to assure good faith performance of the contract may be considered by the Issuing Office, in its sole discretion, for best and final offers or contract negotiation.

PART IV

WORK STATEMENT/REQUIREMENTS

IV-1. Overview

Treasury and its component Bureaus conduct significant ongoing marketing efforts to fulfill the Department's various mandates. The following provides brief summaries of these efforts.

Bureau of Savings Programs

The Bureau of Savings Programs (BSP) oversees three separate but related savings programs for the benefit of Pennsylvania residents.

- **Pennsylvania 529 College Savings Program (PA 529)**-PA 529 oversees two tax-advantaged 529 college savings plans: the PA 529 Guaranteed Savings Plan where growth is based on tuition inflation rather than the financial markets and the PA 529 Investment Plan which offers 16 investment options, ranging from conservative to aggressive, from the Vanguard Group.

PA 529 communicates with more than 130,000 account owner households by mail and email. During its biannual marketing campaigns, PA 529 sends mailings to between 300,000 and 600,000 households and emails approximately 340,000 individuals.

- **Pennsylvania ABLE Savings Program (PA ABLE)**-PA ABLE is a savings plan through which individuals with disabilities and their families can save for disability-related expenses, tax-free, while maintaining their federal and state benefits.

PA ABLE communicates with more than 1,500 account owner households by mail and email. During enrollment drives, PA ABLE contacts over 100,000 prospective account owners via direct mail and over 8,000 prospective account owners through email.

- **Keystone Scholars**-Keystone Scholars is a program that provides a \$100 grant to newborns born to or adopted by Pennsylvania residents. A pilot program was launched in 2018 for residents of six Pennsylvania counties. Beginning in 2019, it will be available to all Pennsylvania residents with children born or adopted after January 1, 2019. When the state-wide program launches, we expect to contact eligible parents via mail and email. Based upon census data, this may result communicating with more than 140,000 households per year.

Bureau of Unclaimed Property

Treasury is responsible for the administration of the Pennsylvania Disposition of Abandoned and Unclaimed Property Act (the Act), 72 P.S. §§ 1301.1-1301.28b, as amended. The realm of unclaimed property is rooted in consumer protection; its explicit goal is to prevent the unjust enrichment by holders of property to which they are not legally entitled, and to establish a process through which lost property may be returned to its rightful owner.

Treasury is under a fiduciary duty to properly account for and safeguard unclaimed monies on behalf of the rightful owner, and ultimately return such monies to the rightful owner. Moreover, all unclaimed property is recorded/held in perpetuity for the rightful owner (presently, this amounts to over \$3 billion). In 2018 calendar year, Treasury received \$278 million of unclaimed monies, and returned \$242 million to rightful owners (encompassing 120,000 claim payments). Treasury sent 103,000 due diligence letters notifying rightful owners. Treasury advertised 104,000 names in 2018. The Bureau of Unclaimed Property answered 126,000 calls to the bureau's Call Center.

Communications Office

The Bureau of Communications and Marketing/ Graphics (BCMG) oversees all public-facing materials and messaging for the department. BCMG regularly distributes press releases to a large and often-changing email list of contacts. BCMG also handles all social media and video content creation and distribution for the department.

IV-2. Products and Services to be Provided

The successful Vendor is expected to provide the following Products and Services. For each Product/Service, **your RFP response must include a detailed description of each and how it will be provided** and then respond to the questions in Section IV-2.B.

A. System Functionality

- **Multi-Channel Advertising.** The System must allow users to create and disperse marketing emails and place and track advertisements and marketing communications sent via email, social media, online search, direct mail, mobile messaging, and other channels.
- **Mail Marketing.** Treasury will use the System to sort data by specific criteria, e.g. zip code, PA 529 GSP account ownership, etc. to generate contact lists for use in mail marketing campaigns.
- **Email Marketing.** Treasury will use the System to send customized emails to various groups including customers and clients of the entities described in Section IV-1. The System must allow Treasury to send unlimited emails to unlimited contacts.
- **Email Automation.** The System must allow users to identify email targets (e.g., new 529 plan enrollees) and automatically send them one or more emails with the ability to utilize conditional variables (e.g., if recipients do not open the email, perform operation A, if they open the email, perform operation B).
- **Centralized Data.** The System must have the ability to combine data sets from different sources (e.g., third party record keeper records, Microsoft CRM, Excel data sheet, purchased

mail/email lists) obtained through different methods (e.g., user-input data, data obtained through an overnight fees, etc.).

- **Behavioral Data.** The System must collect behavioral data (e.g., Google Analytics, Facebook ad performance, Google AdWords performance).
- **Data Scrubbing.** The System must prevent duplicate records and allow users to conduct ongoing list cleaning – so that invalid street addresses (RTS and NCOA) and email addresses can be deactivated and replaced automatically. This functionality must include the ability to incorporate “Do Not Contact” and/or Email Suppression Lists.
- **Categorizing Users.** The System must have the ability to label various users and user groups so that, for example, we know if they are a PA 529 account owner, a PA ABLE account owner, a Keystone Scholars account owner, a community partner for one or more of those programs, a vendor, a lead, etc.
- **Roles for Internal Users.** The System must accommodate a review or decision tree that would allow users to review/approve language used in communications.
- **Gather Data.** The System must allow users to create forms and imbed them in Treasury’s websites in order to gather additional data and have it feed directly into the System. Forms must be easily integrated into existing websites, ADA compatible, HTML5 structure.
- **Behavioral Tracking.** The System must allow users to gather behavioral data by tracking known and unknown Treasury website users.
- **Audience Modeling.** Based on known clients, customers, and other individuals to whom Treasury communicates, the System must allow users to find like audiences and market to them.
- **Data Collection and Analysis.** The System must allow users to see the performance of multi-step campaigns and determine the return on investment for Treasury’s various advertising and marketing efforts. It must have the capacity to track efficacy across many channels including: email, direct mail, and social media/paid digital.
- **User and Data Segregation.** The System must allow users and user groups and data to be kept separate among the entities discussed in Section IV-1.
- **Recordkeeping Platform Interfacing.** The System must interface with Treasury users’ recordkeeping platforms to synchronize contact information in order to avoid duplication of records:
 - **PA 529 and PA ABLE.** PA 529’s recordkeeping platform, Unite, is hosted by its partner, Ascensus College Savings Recordkeeping Services, LLC.
 - **Keystone Scholars.** Keystone Scholars’ recordkeeping platform, Outcome Tracker, is hosted by VistaShare, LLC.
 - **Bureau of Unclaimed Property.** The recordkeeping platform, UPS2000, is hosted by Conduent.
- **Training.** The Vendor must provide ongoing training for Treasury end users and, if applicable, Treasury personnel who will be responsible for System functionality and maintenance.

- **System Security.** The System must employ stringent safeguards to ensure that Treasury data is protected.
- **Ongoing Technical Support.** Technical support must be available during regular business hours and during periods of high demand as described by Treasury.

B. Questions

- Is the System all-inclusive or are additional modules required to be purchased for specific uses/functionality?
 - What uses/functionality requires additional modules?
- As stated in Part I-1, Treasury prefers that the System be housed by the Vendor. Do you propose that the System be housed in Treasury or by the Vendor? What is the reason for your proposal?
 - If the System will be housed in Treasury, for what duties will Treasury personnel be responsible, e.g. maintenance, building functionality within the System, etc.?
 - If the System is housed by the Vendor, provide a detailed description of how this will be accomplished and the safeguards that are in place to ensure the security of Treasury’s data. Refer to the requirements in Appendix F when formulating your response, and specify the requirements, if any, with which you are or will be unable to comply.
- Does the System feature an approval system where, for example, one group of users are permitted to create an email and another group must give approval before the email is sent?
- Does the System allow for integration with CRM, Google Analytics, etc.? Are additional modules or purchases required for this integration?

LIST OF APPENDICES & ATTACHMENTS

Section	Title	Description
Appendix A	Proposal Cover Sheet	Vendor response required
Appendix B	Contractor Integrity Provisions	--
Appendix C	Contractor Responsibility Provisions	--
Appendix D	Nondiscrimination/Sexual Harassment Clause	--
Appendix E	Standard Contract Terms and Conditions	--
Appendix F	Hosted Services Response Acceptability Provisions	

Section	Title	Description
Attachment A	RFP 18-002 Cost Response	Vendor response required

Section	Title	Description

Appendix A
PROPOSAL COVER SHEET
PENNSYLVANIA DEPARTMENT OF TREASURY
RFP 18-002

Enclosed in Three separately sealed submittals is the proposal of the Vendor identified below for the above-referenced RFP:

Vendor Information:	
Vendor Name	
Vendor Mailing Address	
Vendor Website	
Vendor Contact Person	
Contact Person's Phone Number	
Contact Person's Facsimile Number	
Contact Person's E-mail Address	
Vendor Federal ID Number	

Submittals Enclosed and Separately Sealed:	
<input type="checkbox"/>	Technical Submittal
<input type="checkbox"/>	Cost Proposal

<i>Signature</i>	
Signature of an official Authorized to bind the Vendor to the provisions contained in the Vendor's proposal:	
Printed Name:	
Title:	

FAILURE TO COMPLETE, SIGN AND RETURN THIS FORM WITH THE VENDOR'S PROPOSAL MAY RESULT IN THE REJECTION OF THE VENDOR'S PROPOSAL

Appendix B

CONTRACTOR INTEGRITY PROVISIONS

It is essential that those who seek to contract with Treasury observe high standards of honesty and integrity. They must conduct themselves in a manner that fosters public confidence in the integrity of the procurement process.

In furtherance of this policy, Contractor agrees to the following:

1. Contractor shall maintain the highest standards of honesty and integrity during the performance of this contract and shall take no action in violation of state or federal laws or regulations or any other applicable laws or regulations, or other requirements applicable to Contractor or that govern contracting with the Commonwealth.
2. Contractor, its affiliates, agents and employees shall not influence, or attempt to influence, any Commonwealth employee to breach the standards of ethical conduct for Commonwealth employees set forth in the *Public Official and Employees Ethics Act, 65 Pa.C.S. §§1101 et seq.* and the *State Adverse Interest Act, 71 P.S. §776.1 et seq.*, or to breach any other state or federal law or regulation.
3. Contractor, its affiliates, agents and employees shall not offer, give, or agree or promise to give any gratuity to a Treasury official or employee or to any other person at the direction or request of any Treasury official or employee.
4. Contractor, its affiliates, agents and employees shall not offer, give, or agree or promise to give any gratuity to a Treasury official or employee or to any other person, the acceptance of which would violate any statute, regulation.
5. Contractor, its affiliates, agents and employees shall not, directly or indirectly, offer, confer, or agree to confer any pecuniary benefit on anyone as consideration for the decision, opinion, recommendation, vote, other exercise of discretion, or violation of a known legal duty by any Commonwealth official or employee.
6. Contractor, its affiliates, agents, employees, or anyone in privity with him or her shall not accept or agree to accept from any person, any gratuity in connection with the performance of work under the contract, except as provided in the contract.
7. Contractor shall not have a financial interest in any other contractor, subcontractor, or supplier providing services, labor, or material on this project, unless the financial interest is disclosed to Treasury in writing and Treasury consents to Contractor's financial interest prior to Commonwealth execution of the contract. Contractor shall disclose the financial interest to the Commonwealth at the time of bid or proposal submission, or if no bids or proposals are solicited, no later than Contractor's submission of the contract signed by Contractor.
8. Contractor, its affiliates, agents and employees shall not disclose to others any information, documents, reports, data, or records provided to, or prepared by, Contractor under this contract without the prior written approval of the Commonwealth, except as required by the *Pennsylvania Right-to-Know Law, 65 P.S. §§ 67.101-3104*, or other applicable law or as otherwise provided in this contract. Any information, documents, reports, data, or records

secured by Contractor from Treasury or a third party in connection with the performance of this contract shall be kept confidential unless disclosure of such information is:

- a. Approved in writing by Treasury prior to its disclosure; or
 - b. Directed by a court or other tribunal of competent jurisdiction unless the contract requires prior Commonwealth approval; or
 - c. Required for compliance with federal or state securities laws or the requirements of national securities exchanges; or
 - d. Necessary for purposes of Contractor's internal assessment and review; or
 - e. Deemed necessary by Contractor in any action to enforce the provisions of this contract or to defend or prosecute claims by or against parties other than the Commonwealth; or
 - f. Permitted by the valid authorization of a third party to whom the information, documents, reports, data, or records pertain; or
 - g. Otherwise required by law.
9. Contractor certifies that neither it nor any of its officers, directors, associates, partners, limited partners or individual owners has been officially notified of, charged with, or convicted of any felony. Contractor also certifies that neither it nor any of its officers, directors, associates, partners, limited partners or individual owners has been officially notified of, charged with, or convicted of any misdemeanor related to his/her employment, professional status, or status with this or any other company.

Contractor shall immediately notify Treasury's Office of Chief Counsel in writing if and when it or any officer, director, associate, partner, limited partner or individual owner has been officially notified of, charged with, convicted of, or officially notified of a governmental determination of any and all felonies. Contractor shall immediately notify Treasury's Office of Chief Counsel in writing if and when it or any officer, director, associate, partner, limited partner or individual owner has been officially notified of, charged with, convicted of, or officially notified of a governmental determination of any and all felonies or a misdemeanor related to his/her employment, professional status, or status with this or any other company.

10. Contractor certifies that neither it nor any of its officers, directors, associates, partners, limited partners or individual owners has been the subject of any regulatory or civil violations including:
- a. Violation of federal or state antitrust statutes.
 - b. Violation of any federal or state law regulating campaign contributions.
 - c. Violation of any federal or state law regulating hours of labor, minimum wage standards or prevailing wage standards; discrimination in wages; or child labor violations.
 - d. Violation of the *Act of June 2, 1915 (P.L.736, No. 338)*, known as the *Workers' Compensation Act, 77 P.S. 1 et seq.*
 - e. Violation of any federal or state law prohibiting discrimination in employment.
 - f. Debarment by any agency or department of the federal government or by any other state.

- g. Any other crime involving moral turpitude or business honesty or integrity.

Contractor acknowledges that Treasury may, in its sole discretion, terminate the contract for cause upon such notification or when the Commonwealth otherwise learns that Contractor has been officially notified, charged, or convicted.

- 11. If this contract was awarded to Contractor on a non-bid basis, Contractor must, (as required by *Section 1641 of the Pennsylvania Election Code*) file a report of political contributions with the Secretary of the Commonwealth on or before February 15 of the next calendar year. The report must include an itemized list of all political contributions known to Contractor by virtue of the knowledge possessed by every officer, director, associate, partner, limited partner, or individual owner that has been made by:
 - a. Any officer, director, associate, partner, limited partner, individual owner or members of the immediate family when the contributions exceed an aggregate of one thousand dollars (\$1,000) by any individual during the preceding year; or
 - b. Any employee or members of his immediate family whose political contribution exceeded one thousand dollars (\$1,000) during the preceding year.

To obtain a copy of the reporting form, Contractor shall contact the Bureau of Commissions, Elections and Legislation, Division of Campaign Finance and Lobbying Disclosure, Room 210, North Office Building, Harrisburg, PA 17120.

- 12. Contractor shall comply with requirements of the *Lobbying Disclosure Act, 65 Pa.C.S. § 13A01 et seq.*, and the regulations promulgated pursuant to that law. Contractor employee activities prior to or outside of formal Commonwealth procurement communication protocol are considered lobbying and subjects the Contractor employees to the registration and reporting requirements of the law. Actions by outside lobbyists on Contractor's behalf, no matter the procurement stage, are not exempt and must be reported.
- 13. When Contractor has reason to believe that any breach of ethical standards as set forth in law, or in these provisions has occurred or may occur, including but not limited to contact by a Treasury officer or employee which, if acted upon, would violate such ethical standards, Contractor shall immediately notify Treasury's Chief Counsel in writing.
- 14. Contractor, by submission of its bid or proposal and/or execution of this contract and by the submission of any bills, invoices or requests for payment pursuant to the contract, certifies and represents that it has not violated any of these contractor integrity provisions in connection with the submission of the bid or proposal, during any contract negotiations or during the term of the contract.
- 15. Contractor shall cooperate with Treasury in its investigation of any alleged breach of ethical standards and any alleged Contractor non-compliance with these provisions. Contractor agrees to make identified Contractor employees available for interviews at reasonable times and places. Contractor shall provide, or if appropriate, make promptly available for inspection or copying, any information of any type or form deemed relevant to Contractor's integrity and compliance with these provisions. Such information may include, but shall not be limited to,

Contractor's business or financial records, documents or files of any type or form that refers to or concern this contract.

16. For violation of any of these Contractor Integrity Provisions, Treasury may terminate this and any other contract with Contractor, claim liquidated damages in an amount equal to the value of anything received in breach of these provisions, claim damages for all additional costs and expenses incurred in obtaining another contractor to complete performance under this contract. These rights and remedies are cumulative, and the use or non-use of any one shall not preclude the use of all or any other. These rights and remedies are in addition to those the Commonwealth may have under law, statute, regulation, or otherwise.
17. For purposes of these Contractor Integrity Provisions, the following terms shall have the meanings found in this Paragraph 17.
 - a. "Confidential information" means information that a) is not already in the public domain; b) is not available to the public upon request; c) is not or does not become generally known to Contractor from a third party without an obligation to maintain its confidentiality; d) has not become generally known to the public through an act or omission of Contractor; or e) has not been independently developed by Contractor without the use of confidential information of the Commonwealth.
 - b. "Consent" means written permission signed by a duly authorized officer or employee of the Commonwealth, provided that where the material facts have been disclosed, in writing, by pre-qualification, bid, proposal, or contractual terms, the Commonwealth shall be deemed to have consented by virtue of execution of this contract.
 - c. "Contractor" means the individual or entity that has entered into this contract with the Commonwealth, including those directors, officers, partners, managers, and owners having more than a five percent interest in Contractor.
 - d. "Financial interest" means:
 - (1) Ownership of more than a five percent interest in any business; or
 - (2) Holding a position as an officer, director, trustee, partner, employee, or holding any position of management.
 - e. "Gratuity" means tendering, giving or providing anything of more than nominal monetary value including, but not limited to, cash, travel, entertainment, gifts, meals, lodging, loans, subscriptions, advances, deposits of money, services, employment, or contracts of any kind.
 - f. "Immediate family" means a spouse and any un-emancipated child.
 - g. "Non-bid basis" means a contract awarded or executed by the Commonwealth with Contractor without seeking bids or proposals from any other potential bidder or Vendor.
 - h. "Political contribution" means any payment, gift, subscription, assessment, contract, payment for services, dues, loan, forbearance, advance or deposit of money or any valuable thing, to a candidate for public office or to a political committee, including but not limited to a political action committee, made for the purpose of influencing any

election in the Commonwealth of Pennsylvania or for paying debts incurred by or for a candidate or committee before or after any election.

Appendix C

CONTRACTOR RESPONSIBILITY PROVISIONS

For the purpose of these provisions, the term contractor is defined as any person, including, but not limited to, a bidder, Vendor, loan recipient, grantee or lessor, who has furnished or performed or seeks to furnish or perform, goods, supplies, services, leased space, construction or other activity, under a contract, grant, lease, purchase order or reimbursement agreement with the Commonwealth of Pennsylvania (Commonwealth). The term contractor includes a permittee, licensee, or any agency, political subdivision, instrumentality, public authority, or other public entity in the Commonwealth.

1. The Contractor certifies, in writing, for itself and its subcontractors required to be disclosed or approved by the Commonwealth, that as of the date of its execution of this Bid/Contract, that neither the Contractor, nor any such subcontractors, are under suspension or debarment by the Commonwealth or any governmental entity, instrumentality, or authority and, if the Contractor cannot so certify, then it agrees to submit, along with its Bid/Contract, a written explanation of why such certification cannot be made.
2. The Contractor also certifies, in writing, that as of the date of its execution of this Bid/Contract it has no tax liabilities or other Commonwealth obligations, or has filed a timely administrative or judicial appeal if such liabilities or obligations exist, or is subject to a duly approved deferred payment plan if such liabilities exist.
3. The Contractor's obligations pursuant to these provisions are ongoing from and after the effective date of the Contract through the termination date thereof. Accordingly, the Contractor shall have an obligation to inform the Commonwealth if, at any time during the term of the Contract, it becomes delinquent in the payment of taxes, or other Commonwealth obligations, or if it or, to the best knowledge of the Contractor, any of its subcontractors are suspended or debarred by the Commonwealth, the federal government, or any other state or governmental entity. Such notification shall be made within 15 days of the date of suspension or debarment.
4. The failure of the Contractor to notify the Commonwealth of its suspension or debarment by the Commonwealth, any other state, or the federal government shall constitute an event of default of the Contract with the Commonwealth.
5. The Contractor agrees to reimburse the Commonwealth for the reasonable costs of investigation incurred by the Commonwealth for investigations of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the Commonwealth that results in the suspension or debarment of the contractor. Such costs shall include, but shall not be limited to, salaries of investigators, including overtime; travel and lodging expenses; and expert witness and documentary fees. The Contractor shall not be responsible for investigative costs for investigations that do not result in the Contractor's suspension or debarment.
6. The Contractor may obtain a current list of suspended and debarred Commonwealth contractors by either searching the Internet at <http://www.dgs.state.pa.us/> or contacting the:

Department of General Services
Office of Chief Counsel
603 North Office Building

Harrisburg, PA 17125
Telephone No: (717) 783-6472
FAX No: (717) 787-9138

Appendix D

NONDISCRIMINATION/SEXUAL HARASSMENT CLAUSE

The Contractor agrees:

1. In the hiring of any employee(s) for the manufacture of supplies, performance of work, or any other activity required under the contract or any subcontract, the Contractor, each subcontractor, or any person acting on behalf of the Contractor or subcontractor shall not, by reason of gender, race, creed, or color, discriminate against any citizen of this Commonwealth who is qualified and available to perform the work to which the employment relates.
2. Neither the Contractor nor any subcontractor nor any person on their behalf shall in any manner discriminate against or intimidate any employee involved in the manufacture of supplies, the performance of work, or any other activity required under the contract on account of gender, race, creed, or color.
3. The Contractor and each subcontractor shall establish and maintain a written sexual harassment policy and shall inform their employees of the policy. The policy must contain a notice that sexual harassment will not be tolerated and employees who practice it will be disciplined.
4. The Contractor and each subcontractor shall not discriminate by reason of gender, race, creed, or color against any subcontractor or supplier who is qualified to perform the work to which the contract relates.
5. The Contractor shall include the provisions of this Nondiscrimination/Sexual Harassment Clause in every subcontract so that those provisions applicable to subcontractors will be binding upon each subcontractor.
6. The Commonwealth may cancel or terminate the contract and all money due or to become due under the contract may be forfeited for a violation of the terms and conditions of this Nondiscrimination/Sexual Harassment Clause. In addition, the agency may proceed with debarment or suspension and may place the Contractor in the Contractor Responsibility File.

Appendix E

STANDARD CONTRACT TERMS AND CONDITIONS

1. Show Service Purchase Contract number on all invoices and correspondence relating to this contract. Address inquiries concerning the payment of invoices to the Comptroller.
2. The Commonwealth is exempt from all excise taxes imposed by the Internal Revenue Service, and has accordingly registered with the Internal Revenue Service to make tax-free purchases under Registration No. 23740001-K. No exemption certificates are required and none will be issued.
3. The Commonwealth is exempt from Pennsylvania Sales Tax. The Sales and Use Tax Regulations provide that exemption certificates are not required for sales made to government entities. Exemption Certificates will not be issued.
4. Contractor agrees to comply with all applicable laws and regulations of the Commonwealth in carrying out this contract.
5. Contractor, its agents and employees, shall act in an independent capacity and shall not act or be deemed to act as officers, employees or agents of the Commonwealth.
6. Send itemized invoices as directed on contract promptly upon service rendered. Don't include in one invoice items on more than one contract number. (Consider as one contract a consecutive series of service purchase contract forms bearing a single total and number.)
7. Questions concerning this contract should be directed to the Agency Procurement Officer. Any correspondence concerning invoices or the payment of bills should be directed to the "Bill To" address.
8. Regardless of provisions to the contrary found elsewhere in the provisions of this contract, the laws of the Commonwealth of Pennsylvania shall be used in the interpretation of this contract and shall prevail over the laws of any other state in the construction of this contract.
9. Contractor shall not be allowed or paid travel or per diem expenses except as specifically set forth in this contract.
10. Performance of this contract is not assignable without prior written consent of the Commonwealth.
11. The Commonwealth may terminate this contract for its convenience if Commonwealth determines termination to be in its best interest. Contractor shall be paid for work completed.
12. The Commonwealth's obligations are contingent upon appropriation of funds for the contract purpose.
13. In carrying out this contract, the Contractor shall minimize pollution and shall strictly comply with all applicable environmental laws and regulations.
14. This contract and/or attachments constitutes the entire agreement between the parties.

15 In the event of conflict between any of these terms and conditions and any attachment hereto, these terms and conditions shall prevail.

16. Contractor agrees to report and deliver any abandoned or unclaimed property held by Contractor or its agents, subcontractors or assignees, as defined by and in accordance with the Disposition of Abandoned and Unclaimed Property Act (DAUPA), 72 P.S. §1301.1 *et seq.* A negative report must be filed if Contractor determines, after a records review, that there is no reportable unclaimed property. Instructions and assistance in filing the report are available from the Bureau of Unclaimed Property holder hotline at 1-800-379-3999 or via e-mail at unclaimedpropertyreporting@patreasury.gov. Additional information regarding the Pennsylvania Abandoned and Unclaimed Property Program is located at www.patreasury.gov.

ASSIGNMENT OF ANTITRUST CLAIMS

Vendor and the Commonwealth recognize that in actual economic practice, overcharges by vendor's suppliers resulting from violations of state or federal antitrust laws are in fact borne by the Commonwealth. As part of the consideration for the award of this contract, and intending to be legally bound, vendor assigns to the Commonwealth all right, title and interest in and to any claims vendor now has or may hereafter acquire under state or federal antitrust laws relating to the goods or services which are the subject of this contract.

CONTRACTOR RESPONSIBILITY PROVISIONS

1. Contractor certifies that it, its affiliates and subsidiaries are not currently under suspension or debarment by the Commonwealth, any other state, or the federal government.
2. If Contractor enters into any subcontracts under this contract with subcontractors who are currently suspended or debarred by the Commonwealth or federal government or who become suspended or debarred by the Commonwealth or federal government during the term of this contract or any extensions or renewals thereof, the Commonwealth shall have the right to require the Contractor to terminate such subcontracts.
3. The Contractor agrees that it shall be responsible for reimbursing the Commonwealth for all necessary and reasonable costs and expenses incurred relating to an investigation of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the Commonwealth which results in the suspension or debarment of the Contractor.

OFFSET PROVISION FOR COMMONWEALTH CONTRACTS

The Contractor agrees that the Commonwealth may set off the amount of any state tax liability or other debt of the Contractor or its subsidiaries that is owed to the Commonwealth and not being contested on appeal against any payments due the Contractor under this or any other contract with the Commonwealth.

CONTRACTOR INTEGRITY PROVISIONS

1. Definitions

- a. Confidential information means information that is not public knowledge, or available to the public on request, disclosure of which would give an unfair, unethical, or illegal advantage to another desiring to contract with the Commonwealth.
- b. Consent means written permission signed by a duly authorized officer or employee of the Commonwealth, provided that where the material facts have been disclosed, in writing, by prequalification, bid, proposal, or contractual terms, the Commonwealth shall be deemed to have consented by virtue of execution of this agreement.
- c. Contractor means the individual or entity that has entered into this agreement with the Commonwealth, including directors, officers, partners, managers, key employees, and owners of more than 5 percent interest.
- d. Financial Interest means:
 - (1) ownership of more than a 5 percent interest in any business; or
 - (2) holding a position as an officer, director, trustee, partner, employee, or the like, or holding any position of management.
- e. Gratuity means any payment of more than nominal monetary value in the form of cash, travel, entertainments, gifts, meals, lodging, loans, subscriptions, advances, deposits of money, services, employment, or contracts of any kind.

2. The Contractor shall maintain the highest standards of integrity in the performance of this agreement and shall take no action in violation of state or federal laws, regulations, or other requirements that govern contracting with the Commonwealth.

3. The Contractor shall not disclose to others any confidential information gained by virtue of this agreement.

4. The Contractor shall not, in connection with this or any other agreement with the Commonwealth, directly or indirectly, offer, confer, or agree to confer any pecuniary benefit on anyone as consideration of the decision, opinion, recommendation, vote, other exercise of discretion, or violation of a known legal duty by any officer or employee of the Commonwealth.

5. The Contractor shall not, in connection with this or any other agreement with the Commonwealth, directly or indirectly, offer, give, or agree or promise to give to anyone any gratuity for the benefit of or at the direction of request of any officer or employee of the Commonwealth.

6. Except with the consent of the Commonwealth, neither the Contractor nor anyone in privity with him shall accept or agree to accept from, or give or agree to give to, any gratuity from any person in connection with the performance of work under this agreement except as provided therein.

7. Except with the consent of the Commonwealth, the Contractor shall not have a financial interest in any other contractor, subcontractor, or supplier providing services, labor, or material on this project.
8. The Contractor, upon being informed that any violation of these provisions has occurred or may occur, shall immediately notify the Commonwealth in writing.
9. The Contractor, by execution of this agreement and by the submission of any bills or invoices for payment pursuant thereto, certifies and represents that he has not violated any of these provisions.
10. The Contractor shall cooperate fully with an annual audit conducted by Treasury and any additional audits as Treasury determines necessary. The Contractor will provide Treasury with copies of any audits conducted by an independent entity or other state utilizing the Wagers system.
11. For violation of any of the above provisions, the Commonwealth may terminate this and any other agreement with the Contractor, claim liquidated damages in an amount equal to the value of anything received in breach of these provisions, claim damages for all expenses incurred in obtaining another contractor to complete performance hereunder. These rights and remedies are cumulative, and the use or nonuse of any one shall not preclude the use of all or any other. These rights and remedies are in addition to those the Commonwealth may have under law, statute, regulation, or otherwise

NONDISCRIMINATION CLAUSE

During the term of this contract, Contractor agrees as follows:

1. Contractor shall not discriminate against any employee, applicant for employment, independent contractor or any other person because of race, color, religious creed, ancestry, national origin, physical ability, age or sex.

Contractor shall take affirmative action to ensure that applicants are employed, and that employees or agents are treated during employment, without regard to their race, color, religious creed, ancestry, national origin, physical ability, age or sex. Such affirmative action shall include, but is not limited to: employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training.

Contractor shall post in conspicuous places, available to employees, agents, applicants for employment and other persons, a notice to be provided by the contracting agency setting forth the provisions of this nondiscrimination clause.

2. Contractor shall in advertisements or requests for employment placed by it or on its behalf state all qualified applicants will receive consideration for employment without regard to race, color, religious creed, ancestry, national origin, physical ability, age or sex.

3. Contractor shall send each labor union or workers' representative with which it has a collective bargaining agreement or other contract or understanding, a notice advising said labor union or workers' representative of its commitment to this nondiscrimination clause. Similar notice shall be sent to every other source of recruitment regularly utilized by Contractor.

4. It shall be no defense to a finding of noncompliance with this nondiscrimination clause that Contractor has delegated some of its employment practices to any union, training program or other source of recruitment which prevents it from meeting its obligations. However, if the evidence indicates that Contractor was not on notice of the third-party discrimination or made a good-faith effort to correct it, such factor shall be considered in mitigation in determining appropriate sanctions.

5. Where the practices of a union or any training program or other source of recruitment will result in the exclusion of minority group persons, so that Contractor will be unable to meet its obligations under this nondiscrimination clause, Contractor shall then employ and fill vacancies through other nondiscriminatory employment procedures.

6. Contractor shall comply with all state and federal laws prohibiting discrimination in hiring or employment opportunities. In the event of Contractor's noncompliance with the nondiscrimination clause of this contract or with any such laws, this contract may be terminated or suspended, in whole or in part, and Contractor may be declared temporarily ineligible for further Commonwealth contracts, and other sanctions may be imposed and remedies invoked.

7. Contractor shall furnish all necessary employment documents and records to, and permit access to its books, records and accounts by, the contracting agency and the Office of Administration, Bureau of Affirmative Action for purposes of investigation to ascertain compliance with the provisions of this clause. If Contractor does not possess documents or records reflecting the necessary information requested, it shall furnish such information on reporting forms supplied by the contracting agency or the Bureau of Affirmative Action.

8. Contractor shall actively recruit minority subcontractors or subcontractors with substantial minority representation among their employees.

9. Contractor shall include the provisions of this nondiscrimination clause in every subcontract so that such provisions will be binding upon each subcontractor.

10. Contractor's obligations under this clause are limited to Contractor's facilities within Pennsylvania or, where the contract is for purchase of goods manufactured outside of Pennsylvania, the facilities at which such goods are actually produced.

THE AMERICANS WITH DISABILITIES ACT

During the term of this contract, the Contractor agrees as follows:

1. Pursuant to federal regulations promulgated under the authority of The Americans with Disabilities Act, 28 C.F.R. §35.101 *et seq.*, the Contractor understands and agrees that no individual with a disability shall, on the basis of the disability, be excluded from participation in this contract or from activities provided for under this contract. As a condition of accepting and executing this contract, the Contractor agrees to comply with the "General Prohibitions Against Discrimination," 28 C.F.R. §35.130, and all other regulations promulgated under Title II of The Americans with Disabilities Act which are applicable to the benefits, services, programs, and activities provided by the Commonwealth of Pennsylvania through contracts with outside contractors.

2. The Contractor shall be responsible for and agrees to indemnify and hold harmless the Commonwealth of Pennsylvania from all losses, damages, expenses, claims, demands, suits and

actions brought by any party against the Commonwealth of Pennsylvania as a result of the Contractor's failure to comply with the provisions of paragraph 1 above.

NOTICE OF ELECTIONS CODE REPORTING REQUIREMENTS

The Pennsylvania Election Code provides that any business entity which has been awarded a contract on a non-bid basis by the Commonwealth shall file a report of political contributions with the Secretary of the Commonwealth on or before February 15 of each year. The Contractor may obtain a copy of the reporting form (DSEB-504) and other information regarding this requirement from the Department of State, Bureau of Commissions, Elections and Legislation, Division of Campaign Finance and Lobbying Disclosure, Room 210, North Office Building, Harrisburg, Pennsylvania 17120 or by phone at 717-787-5280.

BUDGET IMPASSE

If the Commonwealth has not enacted an annual General Fund budget, which has been passed by the General Assembly and signed by the Governor, on or before the start of the new fiscal year on July 1, the Commonwealth shall be considered to be in a budgetary impasse. Under such circumstances, Contractor shall continue to render services to Treasury through the budgetary impasse and will invoice Treasury for such services. Once the Commonwealth General Fund budget has been passed by the General Assembly and signed by the Governor, Treasury will pay all outstanding invoices as soon as practically possible, but no later than 45 days. If there are no funds appropriate in the enacted General Fund budget to continue this Agreement, then the termination of this Agreement shall be effective, provided, however, Treasury shall pay for all services rendered during the impasse.

Appendix F

HOSTED SERVICES RESPONSE ACCEPTABILITY STIPULATIONS

Data Ownership: The Treasury will own all right, title and interest in its data that is related to the services provided by this procurement contract. The Contractor shall not access Treasury user accounts or Treasury data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract, or (4) at the Treasury's written request.

Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Treasury information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Treasury information and comply with the provisions set forth in this Appendix F, including the following conditions:

- a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.
- b. All data obtained by the Contractor in the performance of this contract shall become and remain property of the Treasury.
- c. All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the personal data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of this procurement contract.
- d. Unless otherwise stipulated, the Contractor shall encrypt all non-public data at rest and in transit. Treasury shall identify data it deems as non-public data to the service provider. The level of protection and encryption for all non-public data shall be identified and made a part of this contract.
- e. At no time shall any data or processes – that either belong to or are intended for the use of Treasury or its officers, agents or employees – be copied, disclosed or retained by the Contractor or any party related to the service provider for subsequent use in any transaction that does not include the Treasury.
- f. The Contractor shall not use any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.

Data Location: The service provider shall provide its services to the Treasury and its end users solely from data centers in the U.S. Storage of Treasury data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Treasury data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Treasury data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in this contract.

Security Incident or Data Breach Notification: The Contractor shall inform the Treasury of any security incident or data breach.

- a. “Incident” means a security event that compromises the integrity, confidentiality or availability of an information asset.
- b. The Contractor shall have an incident response plan and team to assess, escalate, and respond to identified physical and cyber security Incidents that impact or are expected to have an impact on Treasury or any users or visitors utilizing the services provided by Contractor, or which may result in data loss or corruption. Contractor shall review and update this incident response plan annually and as needed throughout the year. Contractor’s incident response team will resolve intrusions and vulnerabilities upon discovery and in accordance with the established procedures.
- c. The Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the Treasury should be handled on an urgent as-needed basis, as part of Contractor communication and mitigation processes as mutually agreed upon, defined by law or contained in the contract.
- d. Security Incident Reporting Requirements: The Contractor shall report a security incident to the appropriate Treasury identified contact immediately as defined in the SLA.
- e. “Breach” means an Incident that results in the confirmed disclosure of data to an unauthorized person or entity.
- f. The Contractor shall adopt a Breach notification and remediation process compliant with applicable law and consistent with best practices. If the Contractor determines that an Incident has led to a Breach, the Contractor will comply with all legal Breach notification requirements under applicable state and federal law and, additionally, follow its Breach notification process. The Contractor’s Incident management and escalation procedures will be adopted by the Contractor and designed to ensure that the Contractor addresses system issues, problems and

security-related events, in a timely manner, and that all Incidents are logged, prioritized, and resolved based on established criteria and severity levels.

- g. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Treasury identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.
- h. If there is a Breach involving Treasury information, the Contractor shall (1) notify Treasury within twenty-four (24) hours of discovery of the Breach, (2) cooperate with Treasury with respect to any such Breach; (3) take appropriate corrective and remedial action to mitigate any risks or damages involved with the Breach to protect Personal Information and other Treasury information from further compromise; (4) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary; and (5) take any other actions that may be required by applicable law as a result of the Breach.
- i. Unless otherwise stipulated, if a data breach is a direct result of the Contractor's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state law; (3) a credit monitoring service required by state or federal law; (4) a website or a toll-free number and call center for affected individuals required by applicable law – all not to exceed the average per record per person cost calculated for data breaches in the United States (currently \$201 per record/person in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute) at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause; all [(1) through (5)] subject to this contract's limitation of liability.

Notification of Legal Requests: The Contractor shall contact the Treasury upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Treasury's data under this contract, or which in any way might reasonably require access to the data of the Treasury. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Treasury without first notifying the Treasury, unless prohibited by law from providing such notice.

Termination and Suspension of Service:

- a. In the event of a termination of the contract, the Contractor shall implement an orderly return of Treasury data in a CSV or another mutually agreeable format at a time agreed to by the parties and the subsequent secure disposal of Treasury data.
- b. During any period of service suspension, the Contractor shall not take any action to intentionally erase any Treasury data.

- c. In the event of termination of any services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Treasury data for a period of:
- 30 days after the effective date of termination, if the termination is in accordance with the contract period
 - 30 days after the effective date of termination, if the termination is for convenience
 - 60 days after the effective date of termination, if the termination is for cause

After such period, unless Treasury agrees to pay a monthly data retention payment to Contractor to continue to retain Treasury data (not to exceed the reasonable hosting cost incurred by Contractor to continue to host such data, but in any event not greater than the average monthly Service fees payable by Treasury over the six (6) months' period preceding expiration or termination of the applicable service agreement), the Contractor shall have no obligation to maintain or provide any Treasury data and shall thereafter, unless legally prohibited, delete all Treasury data in its systems or otherwise in its possession or under its control.

- d. The Treasury shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the SLA.
- e. The Contractor shall securely dispose of all requested data in all of its forms, such as disk, CD/DVD, backup tape and paper, when requested by the Treasury. Data shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the Treasury.

Background Checks: The Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the contract, who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Treasury's information among the Contractor's employees and agents.

Access to Security Logs and Reports: The Contractor shall provide reports to the Treasury in a format as specified in the SLA agreed to by both the Contractor and the Treasury. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all Treasury files related to this contract.

Contract Audit: The Contractor shall audit conformance to the contract terms. The Treasury or a contractor of its choice may perform the audit. The cost of the audit is the responsibility of the Treasury.

Data Center Audit: The Contractor shall perform an independent SOC 2 Type 2 audit annually for all relevant data centers at the Contractor's expense. The audit must be made available to the jurisdiction if requested under unilateral NDA or after being redacted.

Change Control and Advance Notice: The Contractor shall give advance notice (to be determined at the contract time and included in the SLA) to the Treasury of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It shall include a new version number.

The Contractor shall follow documented change management policies and procedures for requesting, testing, and approving application, infrastructure, and product related changes. Changes will undergo various levels of review and testing, including security and code reviews, regression, and user acceptance prior to approval for implementation. Following the successful completion of testing, Treasury must approve changes prior to implementation in a production environment. Dedicated environments separate from production will be made available for development and testing activities. Logical access controls, requiring two-factor authentication, will secure these separate environments. Only authorized individuals can approve an environment being moved into production.

SOC2 Audit Reports. Contractor and its hosting provider shall follow AICPA guidelines and regularly review controls as described in each such party's SOC2 audit report. Contractor will provide Treasury with a copy of its SOC2 independent auditor report upon request, and a copy of any such report made available by Contractor's hosting provider (which may be redacted by such hosting provider to protect confidential information).

Data storage. Contractor will provide recoverable back up of all Treasury data held by it or Contractor's hosting service provider.

Contractor security program:

- **Scope and Contents.** Contractor shall maintain a written security program that (A) complies with applicable industry recognized information security frameworks, (B) includes administrative, technical and physical safeguards reasonably designed to protect the confidentiality, integrity and availability of data and (C) is appropriate to protect Treasury information, taking into account Treasury's important governmental function, and the nature, size and complexity of Treasury's Bureau of Unclaimed Property processes and operations.

- **Security Program Changes.** Contractor has adopted or will adopt, as needed or appropriate, policies, standards, and operating procedures related to security, availability and confidentiality that are available to its personnel. Contractor shall review, update and approve security policies and procedures at least annually to maintain their continuing relevancy and accuracy. Contractor personnel shall acknowledge their understanding and obligation to adhere to security policies at least on an annual basis. Any published Contractor privacy policy(ies) may add to or supplement the requirements set forth in this Appendix, but will be subordinate to and not derogate from such requirements.
- **Security Officer:** Contractor will have a chief privacy officer or other person (or internal group) responsible for adherence to legal and contractual privacy requirements. Such officer or group shall develop, maintain, review, and approve Contractor's security, availability, and confidentiality standards and policies, and insure that Contractor adheres to the requirements of the Contract and this Appendix.
- **Security Training & Awareness:** Contractor personnel shall complete security awareness training on at least an annual basis, and re-acknowledge their receipt of and understanding of Contractor security and privacy policies, as appropriate or necessary to assure compliance with the requirements of the Contract and this Appendix. Contractor shall conduct periodic security awareness programs to educate personnel about their responsibilities and give them direction for creating and helping to maintain a secure workplace.

Risk management: Contractor has or will adopt a formal security risk assessment and management process to identify potential threats to its organization and operations. Contractor management shall rate and review all identified risks.

Access control program: Contractor shall manage access to internal and external applications via Active Directory user security groups, and shall allocate privileges and permissions to users or groups on a least privilege principle. Accordingly, Contractor shall assign application and data rights based on user groups and roles, and shall grant access to information based on job function, all as notified to and approved by Treasury. Contractor shall classify informational assets in accordance with Treasury's data classification requirements, or standardized requirements approved by Treasury.

User access management: Contractor shall require approved access requests prior to granting new user access and changing existing user access to the applicable hosted services, networks and systems. Contractor shall promptly disable application, platform and network access for terminated users upon notification of termination. Contractor shall review access privileges to internal systems and the networks, including administrative access privileges, on a quarterly basis. Contractor shall use separate administrative accounts to perform privileged functions and such access will be restricted to authorized individuals.

Password management and authentication controls: Authorized users must identify and authenticate to the network, applications, and platforms using their unique user ID and password. The system authentication for access to the hosted services and network must follow current NIST Guidelines.

Remote access: If users are able to access applications remotely, Contractor must specify how users will gain this access – e.g., whether two-factor authentication will be used and what other security protection policies or procedures will be instituted to authenticate each user accessing the services.

Asset configuration and security: All Contractor workstations shall have active Endpoint Security software installed to monitor for virus and malware infections. Endpoint devices utilized by Contractor and the hosting service provider shall be scanned in real-time and a full system scan will be performed at least weekly. Monitoring shall be instituted to indicate when an Endpoint Security software does not respond for a prolonged period of time. Contractor shall investigate and take appropriate action to resolve issues. Endpoint Security updates shall be pushed out to endpoint devices automatically from the Endpoint Security software central administration console as they become available. All data storage devices shall use encryption in accordance with cryptography standards referenced in FIPS 140-2, Security Requirements for Cryptographic Modules. IT administrators engaged by Contractor and the hosting service provider shall be alerted of discrepancies in security policies and settings identified from the configuration and management tools utilized by Contractor or the hosting service provider. Contractor shall maintain and regularly update its inventory of infrastructure assets utilized in operating its systems and providing the hosted services, and systematically reconcile the asset list at least annually.

Threat and vulnerability management and security testing: Contractor shall have a Threat and Vulnerability Management (TVM) program to monitor for vulnerabilities on an on-going basis that are acknowledged by vendors, reported by researchers, or discovered internally through vulnerability scans or otherwise. Contractor shall document vulnerabilities with a security risk ticket and rank such vulnerabilities based on severity, which is determined by the likelihood and impact ratings assigned. Contractor shall assign tickets to the appropriate personnel for remediation, and vulnerabilities shall be tracked to resolution. Contractor shall conduct internal and external vulnerability scans at least on a weekly basis, and such scans shall be conducted using an industry-recognized vulnerability scanning tool. Contractor shall evaluate and document identified vulnerabilities within a security risk ticket, and remediate any such vulnerabilities to mitigate or remove the associated risks. Contractor and its hosting provider shall conduct security penetration tests on the hosted services environment(s) at least annually to detect network and application security vulnerabilities. Critical findings from these tests shall be evaluated, documented with a risk ticket, and assigned to appropriate personnel for remediation.

Logging and monitoring: Contractor shall continuously monitor application, infrastructure, network, data storage space and system performance. Contractor's (or its hosting service provider's) monitoring system will receive security log information from servers, firewalls, routers, and Intrusion Detection System devices on a real-time basis. Logs will contain details on the date, time, source, and type of events. Contractor's personnel shall review key reports daily

and follow up on events, as necessary. System logging will be enabled for end user and administrator activity and will be reviewed as necessary, including failed and successful login attempts and updates executed by privileged Contractor system users.

Security: The Contractor shall disclose its non-proprietary security processes and technical limitations to the Treasury such that adequate protection and flexibility can be attained between the Treasury and the Contractor. For example: malware protections, virus checking, data loss protections, intrusion detection, and port sniffing – the Treasury and the Contractor shall understand each other’s roles and responsibilities.

Secure development: Contractor’s software development methodology will govern the acquisition, development, implementation, configuration, maintenance, modification, and management of infrastructure and software components used to make the services available. The methodology will be consistent with the Contractor’s security, availability, and confidentiality policies, as required in the Contract and this Appendix. Contractor’s developers will use secure coding guidelines based on leading industry standards, and receive annual secure coding training. For each new release, Contractor shall perform a security architecture review and conduct a vulnerability scan and static code analysis in the development environment. Identified vulnerabilities and coding defects will be resolved prior to implementation. Prior to final release of a new release of the hosted services for use by Treasury, an internal rollout will be performed within the hosted environment to test and troubleshoot the release. Contractor shall use a code versioning control system to maintain the integrity and security of application source code. Access privileges to the source code repository shall be reviewed periodically by Contractor and limited to authorized employees and subcontractors.

Network security: Network perimeter defense solutions, including an Intrusion Detection System (IDS) and firewalls, shall be used to monitor, detect, and prevent malicious network activity. Security operations personnel will monitor items detected and take appropriate action. Firewall configurations and rules will be reviewed at least annually. Significant changes to firewall rules will follow the Change Management process and require notification to and approval by Treasury. Contractor’s networks will be logically segmented by Virtual Local Area Networks (VLANs) and firewalls will monitor traffic to restrict access to authorized users, systems, and services.

Third party security: Contractor shall assess the risk associated with new vendors prior to onboarding, and shall have an ongoing risk management process for existing vendors. The Contractor shall employ a risk-based vendor scoring model that accounts for data access, network connectivity, compliance impacts and sub-vendor usage among other elements. Contractor shall communicate security and confidentiality requirements and operational responsibilities to third parties through contractual agreements. Contractor shall evaluate physical security controls at each co-location data center on a quarterly basis. This includes reviewing the applicable security assurance reports and contractual obligations. The impact of any issues identified will be assessed by Contractor and, if necessary, remediation shall be instituted and tracked by Contractor, as needed. Contractor shall conduct onsite reviews of contracted data centers on an as-needed basis.

Physical security: Contractor will grant physical access to Contractor facilities (including data centers where access is necessary for certain employees, subject to the requirements of the hosting service provider operating any such data center(s)) based on job responsibilities. Contractor shall remove physical access when access is no longer required and as a component of the employee termination process. Personnel and visitors must display identity badges at all times within Contractor facilities. Contractor shall maintain visitor logs and escort visitors at all times. Badge readers will control access to restricted areas within Contractor facilities and data center locations. Unauthorized badge access attempts will be denied and logged. For data centers that do not require standing-access, access will be granted only for the duration of a data center visit based on an approved access request. Access to data center facilities can only be approved by authorized individuals. Contractor shall review data center physical access, including remote access, on a quarterly basis to confirm that access is restricted to authorized personnel.

Oversight and audit: Contractor shall conduct internal control assessments on a quarterly basis to validate that control are designed and operating effectively. Issues identified from assessments will be documented, tracked and remediated as appropriate. Internal controls related to security, availability, and confidentiality will be audited by an external independent auditor at least annually and in accordance with applicable regulatory and industry standards. Contractor shall document and track the resulting auditor findings for remediation. Independent audit reports shall be made available to Treasury.

Human resources security: Contractor personnel shall be required to sign a confidentiality agreement and acknowledge security policies during the new employee on-boarding process. Contractor shall conduct background verification checks for potential Contractor personnel as required in the Contract and the Appendices thereto, and otherwise in accordance with relevant laws and regulations. Contractor shall maintain a disciplinary process to take action against personnel that do not comply with Contractor's policies and/or procedures, including but not limited to, those put in place to meet its security, availability and confidentiality commitments and requirements.

Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Treasury data to that which is absolutely necessary to perform job duties.

Import and Export of Data: The Treasury shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor. This includes the ability for the Treasury to import or export data to/from other service providers.

Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing, and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

Subcontractor Disclosure: The Contractor shall identify all of its strategic business partners related to services provided under this contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

Right to Remove Individuals: The Treasury shall have the right at any time to require that the Contractor remove from interaction with Treasury any Contractor representative who the Treasury believes is detrimental to its working relationship with the Contractor. The Treasury shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the Treasury signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual. The Contractor shall not assign the person to any aspect of the contract or future work orders without the Treasury's consent.

Business Continuity and Disaster Recovery: The Contractor has adopted or shall adopt a Business Continuity Plan and a Disaster Recovery Plan to manage significant disruptions to the Contractor's operations and infrastructure. The Contractor's chief privacy officer (or equivalent) shall review, update and approve these plans annually. The Contractor shall conduct exercises to evaluate the tools, processes and subject matter expertise of the Contractor in response to a specific incident. The Contractor shall document a summary of the exercise results, and track and remediate any issues identified. The Contractor shall provide the Business Continuity and Disaster Recovery Plans upon request and ensure that the Treasury's recovery time objective (RTO) is met. RTO shall be negotiated by the parties.

Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

Web Services: The Contractor shall use secure Web services to interface with the Treasury's data in near real time when possible.

Encryption and key management: The Contractor shall use industry standard encryption technologies for data contained within, accessed by, or transmitted through the Contractor systems in accordance with appropriate data classification standards. The encryption process used for backup will be subject to Treasury approval. The Contractor shall prevent its employees and subcontractors from storing personal data on portable devices, except within data centers located in the United States. If personal data must be stored on portable devices to accomplish the work, the Contractor must use hard drive encryption in accordance with cryptography standards referenced in FIPS 140-2, Security Requirements for Cryptographic Modules.

The Contractor shall encrypt and secure Treasury's encryption keys within the authority server and securely transfer those keys during the sign-in process. The Contractor shall maintain a policy and process for managing encryption keys for file data blocks, which includes security requirements for key creation, use, storage, and protection. The Contractor shall generate encryption keys using a secure random number generated based on a global industry recognized information security framework.

of Data at Rest:

Model SLA metrics

Metric	Example response
1. Percentage uptime guarantee	99.90%
2. Intervals measured	Every 15 minutes during guaranteed periods.
3. Time periods used for measuring uptime	Monthly, starting each first of month at 12:01am Central Time
4. Committed periods during which uptime is guaranteed	Seven days/week, 2:00am-12:00 midnight; Saturday
5. Exception periods, during which uptime is not guaranteed, in addition to agreed maintenance window.	Examples include: 1. Planned Maintenance 2. *Acts of God 3. Suspension of Service due to legal reasons 4. Internet access outside control of provider
6. Maximum response time (for query & update functions), goal percentage	98 percent within 4 seconds
7. Maximum support response time	*Tier 1 Support issues: 2 hours *Tier 2 issues: 4-6 hours *Tier 3 issues: 12+ hours *Tiers should be defined in SLA and may reflect a scale of standard issues to 'Code Red' service failures
8. Penalty or service credit calculation for recovery point objective failure interruption	5% off a future month service for each consecutive block of 12 hours of failure to meet recovery point objective
Penalty or service credit calculation for service interruption	5% off a future month service for each block of 3 consecutive (at 15-minute intervals) failures to respond within 10 seconds

Attachment A

RFP 18-002 Cost Response