REQUEST FOR PROPOSAL FOR DIGITAL GOVERNMENT SERVICES ISSUED BY THE OFFICE OF THE STATE TREASURER, DEPARTMENT OF STATE AND DEPARTMENT OF TECHNOLOGY AND INFORMATION

CONTRACT NUMBER: TRE20104-DIGITALGOV

I. Overview

By this request for proposal (the "RFP"), the Office of the State Treasurer ("OST"), on behalf of itself and the Cash Management Policy Board (the "Board") the Department of Technology and Information ("DTI"), and the Department of State ("DOS") are seeking proposals for the following products and services:

- Web and application design
- Payment gateway
- Merchant processing and
- Account reconciliation and fee analysis

(collectively, "Digital Government"). Qualified businesses ("Vendors") shall have substantial electronic payment and public sector experience and be incentivized to provide an integrated set of Digital Government services that will result in a simplified online experience for customers accessing State of Delaware ("State") government applications and services.

This RFP is issued pursuant to 29 *Del. C.* §§ 6981, 6982(b) and 6986.

A. Timetable

The tentative timetable for this RFP process is as follows:

EVENT	DATE
RFP published	10/12/2020
Deadline for Vendors' Questions	10/30/2020
Deadline for State Responses - Q&A Closed and Published	11/13/2020
Deadline for Vendors Proposal Submission	12/4/2020 (4:00 PM Eastern time)
Date for Invitation	12/18/2020
Finalist Presentations	Week of 01/11/2021
Finalist Selected / Begin Contract Negotiations	Week of 02/01//2021
Estimated Award Notifications (Board Approval)	Week of 02/15/2021
Complete Contract Negotiations	5/28/2021

There will be no pre-bid meeting associated with this RFP.

This RFP is not an offer. The State reserves the right to cancel this RFP or modify the above RFP dates at any time, and for any reason.

Vendors are expected to fully inform themselves of, and by submitting a proposal shall be deemed to have read, understood and unconditionally and irrevocably accepted, all conditions, requirements, and specifications of this RFP and all attachments and exhibits, subject only to the exception process provided for herein.

B. Proposal to Remain Open

Vendors that submit a proposal in response to this RFP shall be deemed automatically to have consented and irrevocably agreed to keep any such proposal open for six (6) months after the deadline for Vendors' proposal submissions, or for such additional period as the State and any Vendors may agree upon. Rates and fees quoted in a proposal shall remain fixed and binding on the Vendors.

C. Contract Term

The original term of the contract between each successful Vendor and the State shall be five years, with three one-year extension options, each exercisable in OST's sole discretion, subject only to Board approval.

D. Designated Contact:

This RFP process will be managed by OST's Chief Operating Officer (the "Designated Contact"):

Name:	Daniel Madrid
Title:	Chief Operating Officer
Address:	820 Silver Lake Boulevard, Suite 100
City/State:	Dover, DE
ZIP:	19904
Email:	Treasury_RFP@delaware.gov
Phone:	(302) 672-6709

E. Submission of Written Questions

All questions about the RFP shall be submitted to the Designated Contact listed above via e-mail on or before 4:00 p.m., prevailing Eastern time, on October 30, 2020.

Questions should be directly tied to the RFP and asked in consecutive order from beginning to end, following the organization of the RFP. Each question should begin by referencing the RFP page number, heading and subject number to which it relates.

The State will provide written responses to questions from prospective Vendors no later than November 13, 2020. Responses will be placed on http://bids.delaware.gov.

II. Background

A. The Cash Management Policy Board

The Board has statutory authority over the investment and deposit of State funds, including the selection of financial institutions that provide investment and banking services to the State. The

Board is comprised of nine (9) members, including five (5) Delaware citizens appointed by the Governor. The remaining four (4) members are State government officials (the State Treasurer, the Secretary of Finance, the Secretary of State and the Controller General) who serve ex-officio.

The Board has two standing committees – an Investment Subcommittee and a Banking Subcommittee. The Banking Subcommittee has standing authority to address and make recommendations to the full Board with respect to merchant processing and Payment Card Industry ("PCI") compliance issues.

The Board meets at least four times a year. Each standing committee also meets at least four times a year.

The Board historically has approved the selection of merchant processing providers and has proposed guidelines governing the deposit of State agency credit and debit card receipts in settlement accounts.[1]

B. The Office of the State Treasurer

OST serves as the administrative arm of the Board and coordinates all meetings of the Board and its committees. OST also has primary responsibility for gateway services, including the selection of the State's primary gateway vendor, and manages the State's relationships with Board-approved merchant processors and PCI vendors.

C. The Department of Technology and Information, Department of State and Government Information Center

DTI is the central information technology organization of the State with responsibility for providing IT services to agencies and other governmental entities. In addition, DTI also coordinates the strategic direction and standardization of Information Technology across the State executive branch including the adoption, where appropriate, of common technologies, toolsets, and processes/procedures applicable to all agencies of the State. Many of these agencies operate with their own internal and external information technology capabilities with separate funding streams, lifecycles, functional requirements, and compliance guidelines.

Since the early 2000s, the State has operated an online presence comprised of many websites and interactive database-driven applications that provide a wide range of functionality. Today hundreds of websites and online applications are managed by dozens of state agencies, each with a different focus, customer-base, technology platform, and revenue model. Some applications accept online payment while others do not. Many exist primarily to provide information to the public about services offered, while some are designed to perform a specific function for a select user group or business need. Many applications maintain their own online user registries while others use shared credentials made available through centralized authentication and authorization systems. While IT standards promulgated by DTI have helped ensure some uniformity for these applications, the State's technology portfolio should be understood by Vendors as heterogeneous and partially non-standardized when viewed as a single enterprise technology platform.

[1] The guidelines are available here: *Cash Management Policy Board Guidelines [link].*

DTI works with the Department of State's Government Information Center ("GIC") helping citizens connect to their government via the Internet. GIC assists state agencies, divisions, and local governments with the creation and maintenance of their websites and leads the statewide Common Look & Feel ("CLF") branding initiative.

D. Web and Application Design Services

The State maintains a strong interest in providing a single-entry customer experience platform for users that integrates richer capabilities that might be associated with a uniform set of web and mobile experiences. The State desires a new approach that provides existing State websites and applications with opportunities for flexible integration with a central Digital Government portal. Such integration is intended to include uniform online payment, directory/search, forms, and other user experience capabilities that result in a more seamless and unified experience, across all devices, for citizens and business customers. Accordingly, the web and application design services resulting in a Digital Government portal are defined to include work necessary to support and manage the development of a flexible, unified, and interactive online experience for citizens, businesses, and other stakeholders interacting with the State online. Users must have a consistent and intuitive experience across services, can login once to access services anytime, anywhere, from any device and can trust the information or transaction is secure and valid.

E. Payment Gateway

Govolution is the State's principal payment gateway provider since 2001. The contract was previously managed by DTI before being transferred to OST in 2019. In 2018, $1.5 billion of agency credit, debit and ACH payments were transacted through Govolution's payment gateway systems.

Other miscellaneous payment gateways are utilized at certain State agencies to accommodate the differing business needs. Most of the State's payment card hardware is provided by Govolution, though some agencies utilize Fiserv hardware.

F. Merchant Processing Services

Bank of America Merchant Services ("BAMS"), a joint venture between Fiserv, Inc. and Bank of America, N.A., was the State's incumbent merchant processer from 2017 to 2020. As a result of the dissolution of BAMS, the State's merchant processing contract was assigned to Fiserv. Fiserv is now responsible for (i) processing, settling all credit card and debit card transactions, (ii) providing hardware and software solutions to conduct bank card and ACH transactions and (iii) the coordination of PCI compliance requirements between the State and its card brands. The State of Delaware currently has approximately three hundred (300) Merchant Identification Numbers in use by more than twenty (20) departments in more than sixty (60) locations.

The merchant processing contract commenced on December 27, 2017, and the initial term expired on December 26, 2020. OST has exercised one optional one-year extension through December 26, 2021 and has one one-year option remaining.

OST is responsible for ensuring PCI compliance across all State agencies. Technical assistance and network scanning are provided by DTI and state agency resources. For PCI purposes, the State is comprised of eighteen Level 3 and Level 4 merchants. In 2019, OST contracted with CampusGuard, a Qualified Security Assessor ("QSA"), to provide access to a Self-Assessment Questionnaire ("SAQ") portal and agency questionnaire assistance.

G. Account Reconciliation and Fee Analysis

OST has historically utilized various electronic account analysis products for bank and merchant account reconciliation. Collections and disbursement account reconciliation is performed using T-Recs software, and account statement analysis is conducted using SmartAnalysis software, both provided by Trintech, Inc.

III. Scope of Services

The Scope of Services for this RFP is detailed in Appendix B.

IV. Minimum Requirements to Apply

Proposals that do not meet the following minimum requirements, or that do not comply with the specifications or material terms and conditions of this RFP, may be considered non-responsive and rejected. Vendors must clearly demonstrate in their proposals how they meet the following minimum qualifications:

1. Vendors must have at least three (3) years of continuous experience providing the Digital Government services that they propose to supply.
2. Merchant processing and payment gateway Vendors shall be Payment Card Industry Data Security Standards (PCI-DSS) certified/compliant.
3. Vendors shall have at least three (3) years of continuous experience providing Digital Government services to government entities.

The State does not wish to dissuade an otherwise qualified Vendor from submitting a proposal based on the foregoing minimum requirements if legitimate business reasons or industry practices mitigate or eliminate the need for any such requirement. **Vendors who fail to meet a minimum requirement must explain in detail in its response the reason or reasons why the State should excuse non-compliance.** The State shall have discretion to accept or reject any such explanation and waive any minimum qualification requirement.

V. RFP Issuance and Submission of Proposals

A. RFP Issuance

1. Public Notice

Public notice has been provided in accordance with 29 *Del. C.* § 6981.

2. Obtaining Copies of the RFP

This RFP is available in electronic form only and as a courtesy, may be found at the following website:

Delaware Office of Management and Budget at *http://www.bids.delaware.gov/*.

3. Assistance to Vendors with a Disability

Vendors with a disability may receive accommodation regarding the means of communicating this RFP or participating in the procurement process. For more information, contact the Designated Contact no later than ten days prior to the deadline for receipt of proposals.

4. RFP Designated Contact

All requests, questions, or other communications about this RFP shall be made in writing to the Designated Contact. Communications must be submitted electronically to the following email address: Treasury_RFP@delaware.gov.

5. Vendors and Legal Counsel

The State may retain professional services or legal counsel to assist in the review and evaluation of this RFP and the Vendors' responses. Vendors shall not contact the State's professionals or legal counsel on any matter related to the RFP unless so instructed in writing by the Designated Contact. Vendors who make contact in violation of this provision may be disqualified from participation in the RFP process. Exceptions exist only for Vendors currently doing business with the State who require contact with such professionals or legal counsel in the ordinary course of business.

6. Contact with Other State Employees

Direct contact with State employees other than the Designated Contact regarding this RFP is expressly prohibited without prior written consent from the Designated Contact. Vendors who directly contact a State employee in violation of this provision may be disqualified from participation in the RFP process. Exceptions exist only for Vendors currently doing business with the State who require contact with State employees in the ordinary course of business.

7. Organizations Ineligible to Bid

Any individual, business, organization, corporation, consortium, partnership, joint venture, or any other entity currently debarred or suspended from conducting business in the State or any other jurisdiction for any reason may be deemed ineligible to respond to this RFP.

8. Exclusions

The State reserves the right to refuse to consider any proposal from a Vendor who itself or its officers or staff:

a) Has been convicted for commission of a criminal offense as an incident to obtaining or attempting to obtain a public or private contract or subcontract, or in the performance of the contract or subcontract;

b) Has been convicted under state or federal statutes of embezzlement, theft, forgery, bribery, falsification or destruction of records, receiving stolen property, or other offense indicating a lack of integrity or honesty;

c) Has been convicted or has had a civil judgment entered for a violation of any state or federal antitrust statute;

d) Has failed:

i. Without good cause to perform under a consulting contract; or

ii. To perform satisfactorily in accordance with terms of any consulting contract;

e) Has violated ethical standards set out in law or regulation; and

f) Any other cause determined by the State to be serious and compelling, and which undermines confidence in the Vendor's ability to perform independently under any resulting consulting contract.

9. No Press Releases or Public Disclosure

The State reserves the right to pre-approve any news or broadcast advertising releases concerning this RFP, the resulting contract, the work performed, or any reference to the State with regard to any project or contract performance. Any such news or advertising releases pertaining to this RFP or resulting contract shall require the prior express written permission of the State.

10. RFP Not an Offer

This RFP does not constitute an offer by the State.

B. Submission of Proposals

1. Proposal Content

Each proposal must be submitted in writing and respond to the items outlined in this RFP. The State reserves the right to reject any non-responsive or non-conforming proposals.

The State discourages overly lengthy and costly proposals and prefers that they be prepared in a straightforward and concise manner. Unnecessarily elaborate brochures or other promotional materials beyond those sufficient to present a fully responsive proposal are not desired.

Proposals must be realistic and must represent the best estimate of time, materials and other costs, including the impact of inflation and any economic or other factors that are reasonably predictable. The State shall have no responsibility or liability for a Vendor's' failure to accurately estimate the costs or resources required to meet the obligations defined in the proposal.

A Vendor should describe in detail on **Attachment 3** any areas where it will be unable to provide services as requested or required herein. In addition, if a Vendor is able to provide the services exactly as requested or required but believes that there would be benefits (such as cost savings or improved service) to making adjustments to the services outlined, the Vendor should describe the adjustments and the benefits on **Attachment 3**. Acceptance or rejection of any or all exceptions is within OST's sole discretion.

Vendors must respond to all mandatory requirements presented in this RFP. The words "shall," "will," and "must" are used herein to designate mandatory requirements. Failure to respond to a mandatory requirement may, in OST's discretion, result in the disqualification of a Vendor from the RFP process.

2. Proposal Delivery

Proposals must be received before the Proposal Due Date and Time (**no later than 4:00 p.m., prevailing Eastern time, on December 4, 2020**). Responses received after the Proposal Due Date and Time will not be considered.

Upload your proposal at: https://treasurer-delaware.bonfirehub.com/portal

Important Notes:

Logging in and/or uploading the file(s) does not mean the response is submitted. Vendors must successfully upload all the file(s) and MUST click the submit button before the proposal due date and time.

Vendors will receive an email confirmation receipt with a unique confirmation number once the submission has been finalized. This will confirm that the proposal has been submitted successfully.
Each submitted item of Requested Information will only become visible to the State after the proposal due date and time.

If the file is mandatory, you will not be able to complete your submission until the requirement is met.

Uploading large documents may take significant time depending on the size of the file(s) and your Internet connection speed. The maximum upload file size is 1000 MB.

Minimum system requirements: Internet Explorer 11, Microsoft Edge, Google Chrome, or Mozilla Firefox. Java Script must be enabled.

Please contact Bonfire directly at Support@GoBonfire.com or 1(800) 354-8010 ext. 2 for technical questions or issues related to your submission. You can also visit their help forum at https://bonfirehub.zendesk.com/hc.

Any proposal received after the Proposal Deadline shall not be considered.

3. Proposal Modifications

Any changes, amendments or modifications to a proposal must be made in writing, submitted in the same manner as the original response and conspicuously labeled as a change, amendment or modification to a previously submitted proposal. Changes, amendments, or modifications to proposals shall not be accepted or considered after the Proposal Deadline.

4. Proposal Costs and Expenses

The State is not responsible for and will not pay any costs incurred by any Vendor in responding to this RFP, including, but not limited to, costs associated with proposal preparation, printing, and delivery, the interview/presentation process and contract negotiations.

5. Late Proposals

Proposals will be electronically date and time stamped upon receipt. Proposals received after the Proposal Deadline will not be opened or considered.

6. Proposal Opening

Proposals will be opened by State personnel. Any unopened proposals will be returned to the proposing firm. Bonfire will create a public log containing the names of all Vendors that submitted proposals and the dates and times of the State's receipt of each proposal. Unless required by applicable law, the contents of any proposal shall not be disclosed prior to contract award.

7. Non-Conforming Proposals

The State may, in its discretion, reject any non-conforming proposals. Non-conforming proposals are defined as those that do not meet the material requirements of this RFP. The State shall have the authority and discretion to determine whether an RFP requirement is material, or a mere formality or non-substantive requirement.

8. Confidentiality of Documents

Subject to applicable law or the order of a court of competent jurisdiction to the contrary, all documents submitted as part of a Vendors' proposal will be treated as confidential during the evaluation process and will not be available for review by anyone other than the State and their counsel. There shall be no disclosure of any Vendors' information to a competing Vendor prior to award of the contract unless such disclosure is required by law or by order of a court of competent jurisdiction.

The State and its constituent organizations are required to comply with the State of Delaware Freedom of Information Act, 29 *Del. C.* § 10001, *et seq.* ("FOIA"). FOIA requires that the State's records are public records (unless otherwise declared by FOIA or other law to be exempt from disclosure) and are subject to inspection and copying by any person upon written request. Once a proposal is received by the State and a decision on a contract award is made, the content of selected and non-selected Vendors' proposals will likely become subject to FOIA's public disclosure obligations.

The State wishes to create a business-friendly environment and procurement process. As such, the State respects that Vendors desire to protect intellectual property, trade secrets and other confidential business information (collectively referred to herein as "confidential business information"). If a Vendor feels that it cannot submit a proposal without including confidential business information, it must adhere to the following procedure or such proposal may be deemed unresponsive, may not be recommended for selection, and any applicable protection for the Vendors' confidential business information may be lost.

In order to allow the State to assess its ability to protect confidential business information, Vendors will be permitted to designate appropriate portions of their proposal as confidential business information.

Vendors may submit portions of a proposal considered to be confidential business information in a separate, sealed envelope labeled "Confidential Business Information" and include the specific RFP number. The envelope must contain a letter from the submitting Vendors' legal counsel describing the information contained in the documents, representing in good faith that the information is protected from disclosure under FOIA, and briefly stating the reasons that such information is exempt under FOIA.

Upon receipt of a proposal accompanied by such a separate, sealed envelope, the State will open the envelope to determine whether the procedure described above has been followed. A Vendor's allegation as to its confidential business information shall not be binding on the State; rather, the State shall independently determine the validity of any Vendor's designation as set forth in this section. Any Vendors submitting a proposal or using the procedures discussed herein expressly accepts the State's absolute right and duty to independently assess the legal and factual validity of any information designated as confidential business information. Accordingly, Vendors assume the risk that confidential business information included within a proposal may enter the public domain.

9. Sub-Contracting

Subcontracting is not permitted without the State's prior written consent. Any Vendor that submits a proposal contemplating the use of independent contractors or a subcontractor shall identify the purpose for such use, as well as the scope of work and other terms for any such arrangement. All independent contractors and subcontractors must agree in writing to be bound by the terms of the Professional Service Agreement (the "PSA").

10. Discrepancies and Omissions

Vendors are fully responsible for the completeness and accuracy of their proposals, and for examining this RFP and all attachments, exhibits and addenda. Failure to do so will be at the sole risk of Vendors. Should a Vendor find discrepancies, omissions, or unclear or ambiguous language in this RFP, Vendor should seek clarification from the State pursuant to the question and answer process detailed below. Protests based on any discrepancies, omissions, or unclear or ambiguous language will be disallowed if the same have not been timely raised in and preserved through the question and answer process below.

11. RFP Question and Answer Process

OST will allow written requests for clarification of the RFP. Vendors must submit written questions in the format specified below so as to be received by the Designated Contact by 4:00 p.m., prevailing Eastern time, on October 30, 2020. Questions must be submitted electronically to the following email address: Treasury_RFP@delaware.gov.

All questions will be consolidated and answered in a single response that will be posted on the State's website at ***http://www.bids.delaware.gov/*** by 4:00 p.m., prevailing Eastern time, on November 13, 2020, or such other date and time as may be prescribed by the State. Vendors names will not be attributed to questions in OST's response.

Questions should be submitted in a standalone Microsoft Word document in the following format:

Section number
Paragraph number
Page number
Text (of passage being questioned)

Questions that deviate from this format may be rejected by the State, in its discretion.

12. State's Right to Reject Proposals

The State reserves the right to accept or reject any or all proposals or any part of any proposal, to waive defects, technicalities or any specifications (whether they be RFP specifications or contained in a Vendor's response), to assess the merits and qualifications of each proposal and Vendor, to solicit new or modified proposals on the same project, as may be necessary or appropriate or in the best interest of the State.

13. State's Right to Cancel Solicitation

The State reserves the right to cancel this solicitation at any time during the procurement process, for any reason, or for no reason at all. The State makes no commitments, expressed or implied, that this process will result in a contract with any Vendor.

A Vendor's participation in this RFP process may result in the State selecting the Vendor to engage in discussions and negotiations of a formal contract. The commencement of such negotiations does not signify, and may not be interpreted as, a commitment by the

State to execute a contract or continue negotiations. The State may terminate negotiations at any time and for any reason, or for no reason at all.

14. State's Right to Award Multiple Source Contracting

Pursuant to 29 *Del. C.* § 6986, the State may award multiple contracts to two or more Vendors if the State makes a determination that such action is necessary or appropriate or in the best interest of the State.

15. Notification of Withdrawal of Proposal

Vendors may modify or withdraw its proposal by written request, provided that both the proposal and subsequent request is received by the Designated Contact prior to the Proposal Deadline. A withdrawn proposal may be revised and re-submitted and will be considered timely as long as the revised proposal is received by the Proposal Deadline.

All proposals received prior to, and which have not been withdrawn by, the Proposal Deadline shall become firm offers and shall not be revocable after that time.

16. Revisions to the RFP

If it becomes necessary to revise any part of the RFP, an addendum will be posted at ***http://www.bids.delaware.gov***.

17. Exceptions to the RFP

Any exceptions to the RFP or any attachments, exhibits or addenda, along with corresponding explanations and alternatives, must be noted and explained on **Attachment 3** and submitted with a proposal by the Proposal Deadline. Vendors that fail to timely and otherwise adequately preserve and assert exceptions shall be deemed to have waived all such exceptions and related arguments. The State has discretion with respect to the acceptance or rejection of exceptions.

18. Exceptions to the PSA

Attached hereto as **Appendix A** is a standard form of PSA and related exhibits. The terms of the PSA will govern the contractual relationship between a Vendor and the State. Any exceptions to the PSA, along with corresponding explanations and alternatives, must be noted and explained on **Attachment 3**. Vendors shall provide a redlined version of the PSA ("Redline") reflecting all requested changes. Vendors that fail to timely and otherwise adequately preserve and assert exceptions to the PSA shall be deemed to have waived all such exceptions and related arguments. The State has discretion with respect to the acceptance or rejection of PSA exceptions.

19. Award of Contract

The issuance of a contract award ("Award") is subject to approval by the State. The State shall have the sole right to select the successful Vendors and approve the issuance of any Award and the terms of any PSA. The State may (a) approve the issuance of an Award to

a Vendor other than the Vendor who submitted the lowest priced proposal, (b) issue multiple Awards, or (c) withdraw the RFP and issue no Award. No Award or contract resulting from this RFP process shall be effective unless and until authorized by the appropriate State entity.

An Award, if any, will be communicated to the successful Vendors and published only after (a) the State authorizes the issuance of an Award, and (b) the State and each such Vendor executes a formal PSA on terms acceptable to the State. No Vendors will acquire any legal or equitable rights or privileges until the occurrence of both events.

The Award, the PSA and all attachments and exhibits, including all pricing information, and amounts and other details concerning any payments made to a successful Vendor shall be matters of public record subject to disclosure under FOIA.

VI. Proposal Requirements and Evaluation

A. Required Information

1. Vendors shall provide the following information with their proposals in the order listed below. Failure to respond to any request for information within this RFP may result in rejection of the proposal. The proposal will be presented in a spiral-bound book or 3-ring binder, with each completed attachment identified in its own tab.

   a) Tab A: Transmittal Letter.

   b) Tab B: Questionnaire(s). Provide a detailed set of responses to the questions posed in **Attachment 1**. All Vendors must respond to **Attachment 1**. Responses should be both complete and concise.

   c) Tab C: Confidential Information Form. Vendors should identify any material information that is considered confidential using the form of **Attachment 2**. Any information not within this form is automatically subject to FOIA.

   d) Tab D: Exception Form. Provide a detailed listing of any exceptions to the RFP, including all attachments and appendices, including the PSA and its exhibits, using the form included as **Attachment 3**. Successful Vendors who do not take exceptions as required are deemed to have consented and irrevocably agreed to the terms of the RFP.

   e) Tab E: Business References. Provide at least three business references using the form provided in **Attachment 4**.

2. Prior to Award, the successful Vendors shall furnish the State with proof of (i) all necessary business licenses, including a valid State business license, (ii) certification(s) necessary to perform services identified herein, and (iii) proof of insurance required under the PSA attached hereto as **Appendix A**.

B. Proposal Evaluation

1. Initial Screening

The Designated Contact and/or designated OST staff shall perform an initial screening of all proposals submitted by qualified Vendors and evaluate them for timeliness and compliance with the minimum qualifications and other requirements set forth herein. OST shall have discretion with respect to any such determination. Proposals that pass the initial screening shall be forwarded to the Evaluation Team (as defined below) for scoring and evaluation as provided herein.

2. The Evaluation Team

An evaluation team ("Evaluation Team") that may be composed of representatives from OST, DTI, the Board and other State entities will evaluate qualified Vendors' proposals meeting all RFP requirements based on the quantitative and qualitative criteria set forth below. Neither the lowest price nor highest scoring proposal will necessarily be selected. OST may in its discretion remove or add members of the Evaluation Team.

3. Evaluation Criteria

Vendors must review the evaluation criteria below and provide responses that address the criteria. The Evaluation Team will not be able to make assumptions about the Vendors' capabilities; therefore, responses should be detailed and concise within the proposal.

The State has outlined the services it will require in the Scope of Services above. In formulating responses, Vendors are encouraged to suggest additional or modified services in their proposals if such additional or modified services will provide a benefit to the State.

Proposals that meet submission requirements of the RFP will be evaluated and scored based on the criteria and points system set forth in the table below.

Evaluation Criteria	Point Value
Experience and reputation in providing Digital Government systems (i.e., web and application design, merchant processing, payment gateway product, account reconciliation and fee analysis products/services)	20
Capability to design integrated and streamlined Digital Government systems that improve the overall user experience for both internal and external customers	20
Demonstrated ability to assess and improve the State's solution platforms, data security and operational practices related to Digital Government systems, including web and application design, merchant processing, payment gateway and account reconciliation and fee analysis products/services	20

Corporate viability and stability to meet requirements (i.e., facilities, resources, financials, business longevity, stable ownership)	20
Familiarity with public work and its procurement and other requirements	20
TOTAL POINTS	**100**

4. Proposal Clarification

The Evaluation Team may communicate with a Vendor in order to clarify uncertainties or gain better understanding of a proposal. The Evaluation Team may require or permit Vendors to modify or supplement their proposals as a result of such communication. Vendors must provide all requested information in a timely manner, which shall mean on or before any deadline established by the Evaluation Team.

5. Communication with References and Past or Present Clients

The Evaluation Team may communicate with all references provided by a Vendor on **Attachment 4** and may use information gained thereby in the evaluation process. In addition, the Evaluation Team may communicate with any known past or present client of a Vendor outside of the reference list, and any information gained may be used in the evaluation process. Vendors that submit a proposal in response to this RFP shall be deemed to have (a) waived any confidentially or other restrictions that may limit in any way a reference or client's ability to convey information relevant to the evaluation process and (b) to all such communications with references or clients.

6. Oral Presentations

The Evaluation Team, after consultation with the appropriate State entities, may invite selected Vendors to make in-person or virtual oral presentations to the Evaluation Team. Presentations are tentatively scheduled for the week of January 11, 2021. *Any costs associated with oral presentations will be borne by the Vendors.* The State requests that all individuals who are expected to be assigned to this engagement be in attendance.

VII. Contract Process

A. Formal Contract

The Vendor that is selected as the finalist and invited via written notification from the State (the "Invitations") to enter into negotiations concerning Digital Government services will be expected to enter into a formal contract with the State in the form of the PSA attached here to as **Appendix A** (the "Contract"). Vendors' attempt to negotiate pricing or other material Contract terms that were not disclosed and detailed in the Vendors' responses may result in the termination of negotiations with, and/or the disqualification of, such Vendors.

B. Modification of PSA

The State, in its discretion, may consider and accept proposed modifications or additions to the PSA, whether or not raised in an exception, subject to any necessary approvals.

C. Time Frame

A Vendor who receives an Invitation must execute a Contract within twenty (20) business days from the date of the Invitation, unless such period is extended by the State, in its discretion. If no Contract has been executed by the applicable deadline, the State may in its discretion cancel the Invitation and enter negotiations with another Vendor.

D. Inception of Services

Absent OST's prior written request or approval, no Vendor is to begin providing services prior to the issuance of an Award.

E. Cancelation of Award

If a Vendor that receives an Award fails to commence providing consulting services when due under the Contract, the State, without liability, may cancel and annul the Award and terminate any Contract. In such event, an Award under this RFP may be made to another Vendor.

F. Collusion or Fraud

Vendors may not restrain competition by agreement to offer a fixed price, or otherwise. By responding to this RFP, each Vendor shall be deemed to have represented and warranted that: (i) its proposal is not made in connection with any competing Vendor submitting a separate response to this RFP; (ii) its approval is in all respects fair and without collusion or fraud; (iii) the Vendor did not participate in the RFP development process and had no knowledge of the specific contents of the RFP prior to its issuance; and (iv) no employee or official of the State, the Board or OST participated directly or indirectly in the Vendor's proposal preparation.

If at any time, whether prior to or after the issuance of an Award, the State determines that any of the foregoing representations was untrue when made or subsequently became untrue, the State may, without liability, cancel and annul the Award and terminate any Contract. In such event, an Award under this RFP may be made to another Vendor.

G. Lobbying and Gratuities and Contingency Fees

As required by 29 *Del. C.* § 6903(b), the successful Vendor is deemed to have sworn under oath that the Vendor has not employed or retained any company or person to solicit or secure a Contract by improperly influencing the State in this procurement process. In addition, the Vendor represents and warrants that it has not directly or indirectly paid or agreed to pay any person, company, corporation, individual or firm, other than a bona fide employee working primarily for Vendor, any fee, commission, percentage, gift or any other consideration contingent upon or resulting from an Award or Contract.

For breach or violation of the foregoing oath, representation or warranty, the State, in its discretion and without liability, shall have the right to cancel and annul any Award and terminate any Contract, or deduct from the Contract price or otherwise recover the full amount of such commission, percentage, brokerage or contingent fee.

H. Solicitation of State Employees

During the RFP process and for the term of the Contract, Vendors shall not, directly or indirectly, solicit any employee of the State to leave the State's employ in order to accept employment with the Vendors, its affiliates, or any person acting in concert with Vendors, without prior written approval of the State.

VIII. Attachments and Appendices

The following items are provided for use in your response. Attachments are required forms to be submitted with your proposal as described in this RFP. Appendices are provided as additional detail or information to assist in your proposal response.

1. Attachments

Attachment 1	Vendor Questionnaire
Attachment 2	Confidential Information Form
Attachment 3	Exception Form
Attachment 4	Business References

2. Appendices

Appendix A	Form of Professional Services Agreement
Appendix B	Scope of Services

Attachment 1: Vendor Questionnaire

CONTRACT NUMBER: **TRE20104-DIGITALGOV**

Overview of Your Firm

1. Provide the following background of your organization—
    a. Legal name of entity
    b. Legal structure of entity (corp., LLC, LP, etc.)
    c. Company's address
    d. Year Founded
    e. Number of employees
    f. Parent company (or equivalent) or controlling stakeholder
    g. State of incorporation or formation
    h. Core values, mission, and vision statements

2. Provide a brief history of your organization, including your firm's primary business focus, how long you have been providing Digital Government services and your experience providing such services to governmental and municipal entities.

3. Does the firm engage in other business activities, besides Digital Government services? If so, list the business activities your firm provides.

4. Provide professional biographies of key employees and Vendor(s) that would be assigned to this engagement, as well as any relevant training and certifications they possess.

5. What is your firm's process for reassigning personnel assigned to this engagement, either at the State's request or at the instigation of your firm?

6. Please describe your organization's experience with our current Digital Government services providers.

Conflicts & Ethics

7. Describe how your firm identifies and manages potential conflicts of interest.

    a. Are there any areas of potential conflict of interest between other activities of your firm and the services outlined in your response? If so, identify these activities and the potential conflict, and explain the safeguards implemented by the firm to preclude the occurrence of conflicts.

    b. Disclose all third-party business relationships that exist between your firm and the State's current merchant processor, gateway services, qualified security assessor and account analysis/reconciliation services providers.

    c. Does your firm hold or sponsor conferences? If so, describe the fee arrangement with sponsors and clients that attend or present at the conference(s).

d. Does your firm receive fees or other direct or indirect forms of compensation from merchant banking providers? If so, please detail the nature and extent of these relationships.

8. Does your firm have a written code of conduct or set of standards for professional behavior? If yes, explain. How is your code of conduct/ethics monitored and enforced?

Experience and Capabilities

9. Describe your approach to providing and supporting Digital Government systems (i.e. web and application design, merchant processing, payment gateway product, account reconciliation and fee analysis products/services) or similar services including product features/capabilities, system design, user experience, and other information supporting a determination that the proposed solution will meet the needs of citizens and agencies for a single, enterprise Digital Government portal.

10. Report the annual volume of Digital Government Services engagements, for both private and public sector clients for the last six years.

11. Given the information provided to you with this RFP (i.e., the background information, detailed scope of services), provide your initial assessment of the strengths and weaknesses of the State's current merchant services architecture. Specifically, identify the top three areas where you would initially focus your attention to enhance the current business model.

12. Report how your firm distinguishes itself from other Digital Government Services Vendors.

13. Describe your reporting capabilities. Identify to what extent you incorporate quantitative data and qualitative information in your reporting and provide sample reports.

User & Data Security

14. Describe the back-up procedures in case of system failure to meet availability and respond to time requirements.

15. Describe the process used for notification of scheduled and non-scheduled down time.

16. Describe how API integration for State data shall traverse a state API gateway with OWASP top-10 and XML security protections;

17. If applications are accessed over the internet, describe how source network IPs, client certificates and database queries are authenticated and validated;

18. Describe the security measures in place to prevent unauthorized user access, integrity and access of the system(s)/data, and databases, including imported data.

19. Describe the auditing capabilities of proposed system(s).

20. Describe how the system(s) encrypt all State non-public data on all vendor devices, including mobile.

21. Describe how the system(s) may provide for administrator configuration of role-based security access profiles at different levels.

22. Describe how the system(s) supports compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), specifically the Privacy and Security Rules at 45 C.F.R Part 160 and 164, subparts A, C, and E.

23. Describe how the system(s) tracks user access and capture results in an audit log, including the timeframe.

24. Describe your capabilities to support 3rd party risk and compliance assessments.

25. Describe your plan to deliver a comprehensive information security program to protect the state citizen information while hosted within the Vendors Infrastructure.

26. Describe your firewall configuration, or other next generation logical control system to separate layers in the architecture, including firewall rules that may be configured specific to application needs.

27. Describe communication between hosts within your computing environment and how it is evaluated by a network or host-based intrusion detection or prevention system.

28. Describe how communications to and from database(s) are encrypted, secured, and managed.

29. Describe your comprehensive security incident detection and response program, including:
    a. Log collection, correlation and threat intelligence,
    b. Active security event monitoring and attack response, and
    c. Compliance aligned log retention, which the State may reserve the right to request copies of.

30. Provide a detailed explanation of your processing data system security, including an overview of all subcontractors and 3rd parties certified to its systems.

31. Please describe any prior security breaches that have compromised your systems. Include notification process to customers, how this impacted customers and the systems put in place to prevent future similar occurrences.

32. In case of a security breach, what is the process to notify the State and its customers, including timing of notification, form of notification, details outlining the breach and potential loss to our customers, and description of recovery and timing of recovery.

33. Please provide a business and continuity/disaster recovery plan that accounts for incidents rated as moderate to severe in nature and the ability to execute the plan to ensure that

Delaware data can be recovered quickly and completely in the event of a business interruption.

34. Please describe your capability to provide audit reports (SOC 2, etc.) that capture user level interaction such as login/logoff with the system(s).

35. What level of training will you provide to the State for the services proposed, either in person periodically, or virtually on an ongoing basis? Please provide a list of the topics typically covered in the training provided by your organization.

Customer Service

36. Describe your customer service program including the platforms for customer and technical inquiries on an ongoing basis.

37. Describe your platforms and processes for tracking, escalating, and reporting incidents and customer inquiries. Include a description of how you categorize incidents based on severity levels and your service level metrics for the prior three years for issue resolution.

38. Certify that system(s) are operational on a 24 x 7 basis with a minimum of 99.5% availability.

39. Describe your customer satisfaction program and how you measure customer satisfaction.

40. Describe your customer service organizational structure. Describe your approach to assigning customer service resource(s) to our accounts.

41. How do you ensure continuity of service when the primary customer service representative is unavailable?

42. Describe the responsibilities of customer service personnel, including the chain of command and escalation procedures for problem resolution.

43. Describe your capabilities to provide remote support via proxy and through online support forums.

44. Describe your procedures for processing inquiries that require research.

45. Describe your process for providing procedures and communications on regularly scheduled updates and release notes for the solution(s).

46. Describe your technical customer support for computer hardware, software, and communication problems.

Quality Assurance

47. Describe in detail any quality improvement program you have in place. Provide statistics or other available performance data related to the level of service quality, as well as any other data that demonstrates your commitment to quality improvement.

48. What are the key performance measures tracked for your products and services offered, what is the reporting frequency and period covered for each measure and what are your last three performance levels for each measure?

49. Are results of the performance measurement published or otherwise made available? Discuss.

50. Do you maintain an internal scorecard that is shared with clients, and if so, please provide a copy in your response to this RFP.

Legal & Regulatory

51. Has your organization been involved in any investigation, examination, complaint, disciplinary action or other proceeding relating to or affecting the firm or its employees' ability to perform its duties under any engagement during the previous five (5) years? If so, describe.

52. Has any person in your organization been involved in providing services been convicted of a felony, found liable in a civil or administrative proceeding, pleaded no contest, or agreed to any consent decree with respect to any matter involving a breach of trust, breach of fiduciary duty, fraud, securities law violations or bankruptcy law violations during the previous five (5) years? If so, describe.

Implementation Plan

53. Provide details on your experience with project management planning and execution based on industry best practices and the Project Management Institute (PMI).

54. Provide a proposed project plan for the system implementation project in response to the RFP, including phases with timetable, major milestones and benchmarks, activities, resources, and contingencies.

55. Provide an overview of any business consulting, coaching, mentoring services and strategies related to this project to aid in user adoption of the solution(s).

56. Provide an overview of your training plan for implementation, ongoing user support, and system upgrades, and include sample training material.

Pricing Proposal

Please propose a fee structure for the services described in **Appendix B** for the initial contract period and any extension periods for each of the components being submitted in the Vendors' proposal. Vendors may provide pricing models that allow convenience fees to be passed through to customers for credit card usage according to current card association rules. Include all maintenance, transaction-based, subscription, user, license, fixed, and upgrade fees that may accompany any component in the Vendors' proposal.

Attachment 2: Confidential or Proprietary Information Form

CONTRACT NUMBER: **TRE20104-DIGITALGOV**

☐ By checking this box, Vendor acknowledges that its proposal does not contain any information it declares to be confidential or proprietary for the purpose of production under FOIA.

Confidentiality or Proprietary Information

Note: Use additional pages as necessary.

Attachment 3: Exception Form

CONTRACT NUMBER: **TRE20104-DIGITALGOV**

Proposals must include all exceptions to the specifications, terms or conditions contained in this solicitation, including all attachments and appendices. If Vendor is submitting the proposal without exceptions, please state so below.

☐ By checking this box, Vendor acknowledges that it takes no exception to the specifications, terms or conditions found in this solicitation, including the terms of the PSA.

Paragraph # and page #	**Exceptions to specifications, terms or conditions**	**Proposed alternative**

Note: Use additional pages as necessary.

Attachment 4: Business References
CONTRACT NUMBER: TRE20104-DIGITALGOV

List a minimum of four business references. At least two (2) of the references should be from government entities. Business references should include the following information:

- Business name and mailing address
- Contact name, phone number and email address
- Number of years doing business with
- Type of work performed

Please do not list any State entity, officer or employee as a business reference.

If you have held a State contract within the last 5 years, provide a separate list of the contract(s), describe the scope of work performed and include the name, title, phone number and email address for your primary contact for each engagement.

APPENDIX A: PROFESSIONAL SERVICES AGREEMENT

This Professional Services Agreement (the "Agreement") is entered into by and between the Office of State Treasurer ("OST") for the State of Delaware (the "State"), on behalf of itself and the Cash Management Policy Board (the "Board"), the Department of Technology and Information ("DTI"), the Department of State ("DOS") and [_____] ("Vendor").

WHEREAS, in October 2020, the State, issued a formal Request for Proposals (the "RFP") pursuant to the State Procurement Code seeking proposals from qualified consulting firms to provide independent Digital Government Services[2] to the State;

WHEREAS, the State desires to obtain from Vendor Digital Government Services as set out in the Statement of Work on **Exhibit 1** to this Agreement;

WHEREAS, Vendor desires to provide such services to the State on the terms set forth in the Agreement;

WHEREAS, OST, on behalf of itself and the Board, DTI, and Vendor represent and warrant that each party has full right, power and authority to enter into and perform under this Agreement;

FOR AND IN CONSIDERATION OF the premises and mutual agreements herein, OST, DTI and Vendor agree as follows:

1. Services and Term.

1.1. Vendor shall provide to the State those services as set forth herein and as specified on the Statement of Work attached hereto as **Exhibit 1** (collectively, the "Services").

1.2. The initial term of this Agreement shall begin on the date this Agreement is fully executed, or as may be otherwise agreed upon by the parties and shall extend for five years from that date. The State has three one-year extension options. OST, in its discretion, may exercise each option at any time prior to the expiration of the initial or extended term, as the case may be, subject only to Board approval of any such extension.

1.3. Vendor shall meet and confer with OST, the Board and/or any committee of the Board at such times and places as OST, the Board or a committee may reasonably request. Vendor, if requested by OST, shall participate in meetings with other State agencies concerning Digital Government Services-related issues. Vendor shall keep OST staff informed of progress and provide updates on the status of the Services. This interface shall include regular telephone communication, exchange of written data and analysis and other interaction as requested by OST.

2. Payment for Services and Expenses.

2.1. OST will pay Vendor for the performance of Services in accordance with **Exhibit 2**.

[2] Capitalized terms used but not defined in this Agreement shall have the meanings ascribed to such terms in the RFP.

2.2. OST's obligation to pay Vendor for the performance of Services will not exceed the annual fixed price and/or rates and limits set forth on **Exhibit 2**. Vendor is solely responsible for ensuring that all Services are completed for the agreed upon price and/or rates and within any applicable cap. Annual fees and/or rates shall be fixed for the initial term of the Agreement and, at OST's option, shall remain fixed for any extension period.

2.3. Unless otherwise agreed, all payments will be sent to Vendor's identified address on record with OST.

2.4. Vendor shall submit invoices to OST in arrears on a monthly basis. Services provided for a fixed annual price shall be prorated and billed monthly. OST agrees to pay undisputed amounts within 30 days of receipt. In the event that OST disputes all or any portion of an invoice, OST agrees to provide Vendor with a detailed statement of OST's position on the invoice, or disputed portion of the invoice, within 30 days of receipt.

2.5. All expenses incurred in the performance of the Services are Vendor's responsibility. Vendor shall not be reimbursed for any expenses incurred by Vendor in the performance of the Services, including, but not limited to, travel and lodging expenses, communications charges, and computer time and supplies.

2.6. OST shall not be liable for the payment of federal, state and local sales, use and excise taxes, including any interest and penalties from any related deficiency, which may become due and payable by Vendor as a consequence of this Agreement.

2.7. OST shall have the right to setoff or subtract from any payment to be made to Vendor all damages, costs and expenses caused by Vendor's breach of the Agreement, or Vendor's negligence, gross negligence or other tortious or illegal conduct in connection with the provision of Services hereunder, to the extent such damages, costs and expenses have not otherwise been reimbursed by Vendor.

2.8. Invoices shall be submitted electronically to OST's Chief Operating Officer, Daniel Madrid at Daniel.Madrid@delaware.gov with a copy to OST Director of Operations and Fund Management, Fiah Kwesseu at Fiah.Kwesseu@delaware.gov.

3. [Reserved.]

4. Responsibilities of Vendor.

4.1. Vendor shall be responsible for the professional quality, technical accuracy, timely completion, and coordination of all Services. In performing the Services, Vendor shall follow practices consistent with generally accepted professional and technical standards and comply with all applicable federal, state and local laws, ordinances, codes and regulations.

Technology Terms & Conditions

1. On Premise Solutions

For on premise solutions, Vendors shall be responsible for ensuring that all services, products and deliverables furnished to the State are consistent with practices utilized by,

or policies and standards promulgated by, the Department of Technology and Information (DTI) published at http://dti.delaware.gov/information/standards-policies.shtml.

2. Cloud Solutions

For cloud solutions Vendors shall comply with the Cloud Services Terms and Conditions, and Data Usage Terms and Conditions Agreements pursuant to Exhibits 3 and 4 of this Agreement.

4.2. [Reserved.]

4.3. [Reserved.]

4.4. [Reserved.]

4.5. It shall be the duty of Vendor to assure that all Services and deliverables are technically sound and in conformance with all applicable federal, state and local statutes, codes, ordinances, resolutions and other regulations applicable to the Services. Vendor will not provide access to software, or produce work product, that violates or infringes on any copyright, trademark, patent or other intellectual property rights. Vendor shall, without additional compensation, correct or revise any errors or omissions in the software or work product and shall indemnify the State and its officers, employees and attorneys for all liability, suits, actions or claims, together with all reasonable costs and expenses (including attorneys' fees), incurred by the State or its officers, employees or attorneys resulting from or attributable to Vendor's failure to comply with this Section.

4.6. OST's review, approval, acceptance, or payment for any Services shall not be construed to operate as an admission or acknowledgement of any fact or circumstance, or a waiver of any rights under this Agreement or otherwise, and Vendor shall be and remain liable in accordance with the terms of this Agreement and applicable law for all damages caused by Vendor's breach or negligent performance or failure to perform under this Agreement.

4.7. Vendor shall appoint a senior employee who will manage the performance of Services and act as the single point of contact to OST.

4.8. Upon receipt of written notice from OST that an employee of Vendor is unsuitable for good cause, Vendor shall remove such employee from the performance of Services and substitute in his/her place an employee suitable to OST.

4.9. Unless legally prohibited, Vendor shall promptly notify OST in writing of any investigation, examination or other proceeding involving Vendor, or any key personnel or designated staff of Vendor, including a contract employee or a subcontractor, or any key personnel or designated staff of a subcontractor, commenced by any regulatory or law enforcement agency and involving allegations of fraud or illegal conduct, or a data breach.

4.10. Vendor agrees that its senior employee and other key personnel or designated staff will cooperate with OST in the performance of Services and will be available for consultation with OST upon reasonable request.

4.11. [Reserved.]

4.12. [Reserved.]

4.13. Vendor has or will retain such employees as it may need to perform the Services.

4.14. Vendor will not use OST's, the Board's or the State's name, either express or implied, in any of its advertising or sales materials without OST's prior written consent.

4.15. Vendor represents that it is properly licensed, registered and authorized to transact business and perform Services in the State.

4.16. Vendor will provide to OST audited or unaudited financial statements, as requested by OST.

4.17. Vendor shall be independent and shall provide advice and recommendations to OST and the Board free of any conflicts of interest and solely in the best interest of the State.

5. OST Responsibilities/Representations.

5.1. OST agrees that its officers and employees will cooperate with Vendor in the performance of Services and will be available for consultation with Vendor upon reasonable request.

5.2. OST shall pay for the Services as provided on **Exhibit 2**, subject to review for compliance with and the terms of this Agreement.

6. Ownership of Work Product and Data and Documents.

6.1. All materials, information, documents, reports and other work product, whether finished, unfinished, or draft, developed, prepared or completed by Vendor relating to the Agreement shall become the property of the State and shall be delivered upon request by OST. The State shall have the right to reproduce and disclose all work product related to this Agreement. The State's rights under this Section shall survive termination of the Agreement.

6.2. The State shall have and retain title and interest to all data and documents related to this Agreement, including Vendor work product and data and documents electronically stored by Vendor. Upon termination of the Agreement, and for a period of six (6) months thereafter, OST shall have the right to request and shall, at OST's option and at Vendor's expense, be provided with copies of all data and documents electronically stored by Vendor related to the Agreement. Promptly after such six (6) month period, all State data and documents shall be destroyed or retained in accordance with Section 7.8.

7. Confidential Information of the State.

7.1. "Confidential Material," as used herein, means all documents and data that contain confidential commercial, financial, consumer, or other confidential information of the State,

whether or not such agreements or other documents are marked "confidential" or otherwise designated as confidential by OST.

7.2. Confidential Material shall be used by Vendor solely for purposes of executing its duties and obligations under the Agreement. Vendor may disclose Confidential Material only to those Vendor employees who have a need to access Confidential Material in the scope of their employment for Vendor, and who have been informed, understand and acknowledge in writing that Confidential Material is highly sensitive and confidential and must be held in strictest confidence.

7.3. Confidential Material shall not be copied or reproduced without the express written permission of OST, except for such copies as may reasonably be required for Vendor to execute its duties and obligations under the Agreement. Except as contemplated by the Agreement, Vendor shall not store or aggregate in a data base or other electronic storage means any Confidential Material; provided, however, that Vendor is permitted to store Confidential Material in physical or electronic files in accordance with this Section 7 while executing its duties under the Agreement and for a reasonable period of time thereafter, after which the Confidential Materials, including all physical and electronic copies, shall be destroyed or retained in accordance with Section 7.8.

7.4. Except as expressly permitted in this Section 7, Confidential Material shall not be disclosed to any individuals or third parties without the prior written consent of OST, unless such disclosure is required by law. Vendor shall immediately notify OST in writing of Vendor's receipt of a court order, subpoena or discovery requests seeking or ordering the production, disclosure or inspection of any Confidential Material. Vendor shall, at the request of OST, object to any such order, subpoena or discovery and shall take all other measures that may reasonably be necessary to protect against the unwarranted production, disclosure or inspection of Confidential Material. In the event disclosure of Confidential Material is compelled or otherwise required by law, Vendor shall mark all documents submitted in connection with any such disclosure so as to indicate the confidential nature of the material and OST's interest therein.

7.5. This Section 7 shall not restrict the disclosure or use of Confidential Material that:

a. is in the public domain at the time of disclosure or thereafter enters the public domain through no breach of the Agreement;

b. is in the possession of Vendor without restrictions when received;

c. has been lawfully obtained or is lawfully obtainable without restrictions from a source other than OST, the Board or the State through no breach of the Agreement;

d. has been developed independently by Vendor and without reliance upon Confidential Material.

7.6. Vendor shall take reasonable steps to restrict access to and otherwise safeguard the confidentiality and integrity of Confidential Material at all times, including, without limitation, the implementation of electronic security procedures and other measures designed to ensure that all Confidential Material is properly stored, and password protected at all times.

7.7. Vendor shall immediately disclose to OST the discovery of any security breach or suspicious intrusion involving Confidential Material and shall identify the type and amount of Confidential Material that was compromised or disclosed.

7.8. Within six (6) months from the termination of the Agreement, all Confidential Material, regardless of form, shall be permanently deleted or destroyed in accordance with all applicable law, orders, rules and regulations and industry best practices. Any electronic data or documents deleted under this Section 7.8 shall be permanently deleted and shall not be recoverable, according to the National Institute of Standards and Technology's approved methods. If requested, Vendor shall provide a destruction certificate to OST listing the type and contents of electronic records or physical documents destroyed or permanently deleted under this Section 7.8. Notwithstanding the foregoing, Vendor may, subject to Vendor's confidentiality obligations under this Agreement, retain copies of State data and documents to the extent required by applicable state or federal law, regulations, rules, or orders or Vendor's document retention policy.

7.9. The State shall have no obligation to disclose Confidential Material. OST may, in its discretion, provide or refuse to provide Confidential Material requested by Vendor.

7.10. Vendor understands and agrees that the State may suffer irreparable harm in the event that Vendor fails to comply with its obligations hereunder and that monetary damages may not be adequate to compensate the State for such breach. Vendor agrees that the State, in addition to other remedies available to it at law or in equity for actual damages, shall be entitled to seek injunctive relief to enforce the terms of this Section 7.

7.11. Vendor's confidentiality obligations shall survive termination of the Agreement.

8. Warranty.

8.1. Vendor agrees to correct or re-perform any Services not in compliance with this Agreement in a timely manner.

8.2. Third-party products within the scope of this Agreement, if any, are warranted solely under the terms and conditions of the licenses or other agreements by which such products are governed. With respect to all third-party products and services purchased by Vendor in connection with the provision of the Services, if any, Vendor shall pass through or assign to the State all rights Vendor obtains from the manufacturers and/or vendors of such products and services (including warranty and indemnification rights), to the extent that such rights are assignable.

9. Indemnification; Limitation of Liability.

9.1. Vendor shall indemnify and hold harmless OST, the Board, the State and their respective officers, members, employees and attorneys ("Indemnified Parties") from any and all liability, suits, actions, claims or damages, together with all reasonable costs and expenses (including attorneys' fees), arising out of Vendor's breach of the Agreement, or the negligent, reckless, intentional or other tortious, fraudulent, illegal, or unlawful conduct of Vendor or any subcontractor, or their respective officers, employees, contract employees or agents, arising out of or related to this Agreement ("Claims").

9.2. If OST notifies Vendor in writing of a Claim against an Indemnified Party, including, without limitation, any Claim based on Vendor's disclosure of or failure to safeguard any personal financial or other Confidential Material, Vendor will defend such Claim at Vendor's expense if so requested by OST, in OST's sole discretion. Vendor will pay any costs or damages that may be finally awarded against an Indemnified Party.

9.3. Except for fees that may be due and owing as set forth in Section 2 above and **Exhibit 2** hereto, and notwithstanding anything to the contrary in this Agreement, neither OST, the Board or the State, nor any officers, members, employees or attorneys of the foregoing, shall have any liability to Vendor or any other party for fees (including attorneys' fees), expenses, suits, actions, claims or damages, whether direct or indirect, compensatory or punitive, actual or consequential, in or for actions, claims, causes of action or rights, including alleged indemnification rights, arising out of or related in any way to this Agreement.

9.4. Notwithstanding anything to the contrary herein, no provision of this Agreement shall constitute or be construed as an indemnification obligation in favor of Vendor, or a waiver or limitation of any right of OST, the Board or the State that may exist under applicable law.

9.5. Notwithstanding anything to the contrary herein, to the extent available under applicable law, OST, the Board and the State, and their respective officers, members, employees and attorneys, expressly reserve all rights, claims, arguments, defenses and immunities, including, without limitation, claims or defenses based on sovereign immunity, qualified immunity and other statutory or common law rights, claims, defenses or immunities; provided, however, that Vendor shall have the right to seek to enforce this Agreement in the courts of this State.

10. Insurance.

10.1. Vendor shall maintain the following insurance during the term of this Agreement:

a. Worker's compensation and employer's liability insurance in accordance with applicable law;

b. Comprehensive general liability - $1,000,000 per occurrence/$3,000,000 per aggregate;

c. Professional liability - $5,000,000 per occurrence/$5,000,000 per aggregate;

d. Automotive liability insurance covering all automotive units used in the work with limits of not less than $100,000 for each person and $300,000 for each accident as to bodily injury and $25,000 as to property damage to others; and

e. Cyber Liability – Vendor must maintain cyber security liability insurance coverage with limits of $30,000,000 per incident for loss resulting from a data breach. The policy shall be issued by an insurance company with an A.M. Best Rating of A-VII and shall remain in place for the term of the Agreement. At a minimum, the policy must include third-party coverage for credit monitoring, notification costs to data breach victims, and regulatory penalties and fines (to the extent insurable). Vendor shall be responsible for any deductible or self-insured retention contained in the insurance policy.

f. Excess/Umbrella policy - Excess/Umbrella $[in an amount TBD] total (sits above underlying worker's compensation and employer's liability, general liability, and automotive liability).

10.2. Should any of the above-described policies be cancelled before the expiration date thereof, notice will be delivered to OST.

10.3. Before any work is performed pursuant to this Agreement, certificate of insurance and/or copies of the insurance policies specified in Section 10.1 shall be provided to OST. The certificate holder is as follows:

Office of the State Treasurer
820 Silver Lake Blvd., Suite 100
Dover, DE 19904

10.4. In no event shall OST, the Board or the State, or their respective officers, members, employees or attorneys, be named as an additional insured on any policy required under this Agreement.

11. Independent Contractor.

11.1. It is understood that in the performance of the Services, Vendor is an independent contractor, not an agent or employee of OST, the Board or the State, and shall furnish such Services in its own manner and method, except as required by this Agreement.

11.2. Vendor has and shall retain the right to exercise full control over the employment, direction, compensation and discharge of all persons employed by Vendor in the performance of the Services; provided, however, that Vendor will, subject to scheduling and staffing considerations, attempt to honor OST's request for specific individuals.

11.3. Vendor shall be solely responsible for, and shall indemnify, defend and hold OST, the Board and the State, and their respective officers, members, employees and attorneys, harmless from all matters relating to the payment of Vendor's employees, contract employees, subcontractor or subcontractor's employees, including compliance with Social Security withholding and all other wages, salaries, benefits and taxes of any nature whatsoever.

11.4. Vendor acknowledges that Vendor and any agents or employees employed or contracted by Vendor shall not, under any circumstances, be considered employees of OST, the Board or the State, and that they shall not be entitled to any of the compensation, benefits or rights afforded employees of the State, including, but not limited to, sick leave, vacation leave, holiday pay, pension benefits, and health, life, dental, long-term disability and workers' compensation insurance benefits.

11.5. Vendor shall be responsible for providing liability insurance for its personnel and agents.

11.6. As an independent contractor, Vendor has no authority to bind or commit OST, the Board or the State. Nothing herein shall be deemed or construed to create a joint venture, partnership, or fiduciary or agency relationship between the parties for any purpose.

12. Suspension.

12.1. OST may for any reason suspend performance by Vendor under this Agreement for such period of time as OST, in its discretion, may prescribe by providing written notice to Vendor. Upon receipt of such notice, Vendor shall not perform further work under this Agreement until Vendor's receipt of written notice from OST to resume performance.

12.2. OST shall pay Vendor compensation earned through the effective date of suspension, less all previous payments and subject to any rights of offset or recoupment that the State may have against Vendor.

13. Termination.

13.1. This Agreement may be terminated by either party for default, which shall mean the failure of the other party to fulfill a material obligation under this Agreement, through no fault of the terminating party, but only after the other party is given:

a. Not less than 14 calendar days' written notice of intent to terminate; and

b. An opportunity for consultation with the terminating party prior to termination.

13.2. This Agreement may be terminated in whole or in part by OST for its convenience, but only after Vendor is given 30 calendar days' written notice of intent to terminate.

13.3. If termination is effected, OST will pay Vendor that portion of compensation earned for Services provided as of the effective date of termination, but:

a. No amount shall be allowed for anticipated profit on unperformed Services or other work;

b. Any payment due to Vendor at the time of termination may be adjusted or reduced to the extent of the State's offset or recoupment rights; and

c. In the event Vendor ceases conducting business, OST shall have the right to make an unsolicited offer of employment to any officers or employees of Vendor.

13.4. In connection with any notice issued under this Section 13, OST may immediately retain another vendor to perform the Services. Vendor shall at all times cooperate in the transition and shall perform such Services and additional services as OST shall determine are necessary or appropriate to enable the transition of work to a successor vendor or vendors. Vendor's obligation to provide transition services shall survive termination and shall continue until such date as is communicated in writing to Vendor that such Services or additional services are no longer needed.

13.5. If after termination for breach it is determined that Vendor has not so failed, the termination shall be deemed to have been effected for convenience.

13.6. The termination of this Agreement shall not terminate indemnification or confidentiality rights or obligations, or any other rights or obligations that are intended to or customarily extend beyond termination.

13.7. The rights and remedies of OST provided in this Section are in addition to any other rights and remedies provided by law or under this Agreement.

13.8. Gratuities.

a. OST may, by written notice to Vendor, terminate this Agreement without liability if it is found that gratuities (in the form of entertainment, gifts, or otherwise) were offered or given by Vendor or any agent or representative of Vendor to any officer or employee of OST, the Board or the State with a view toward securing a contract or securing favorable treatment with respect to the awarding or amending or making of any determinations with respect to the performance of this Agreement.

b. In the event this Agreement is terminated as provided in Section 13.8.a, the State shall be entitled to pursue the same remedies against Vendor it could pursue in the event of a breach of this Agreement by Vendor.

c. The rights and remedies of OST, the Board and the State provided in Section 13.8 shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Agreement.

13.9. Validity and enforcement of this Agreement is subject to appropriations by the General Assembly of the specific funds necessary for contract performance. If such funds are not so appropriated, (a) OST may immediately terminate this Agreement without liability, and (b) the Agreement shall be terminated without liability as to any obligation of OST requiring the expenditure of money for which no specific appropriation is available.

14. Assignment; Subcontracts.

14.1. Any attempt by Vendor to assign or otherwise transfer any interest in this Agreement without the prior written consent of OST shall be void.

14.2. Vendor's employees shall perform all Services, unless OST consents in writing to Vendor's request to use temporary staff, independent contractors or a subcontractor. Neither approval by OST of any such request, nor OST's acceptance of any software, deliverable or payment of any invoice, shall relieve Vendor of responsibility for the professional and technical accuracy and adequacy of the Services. All temporary staff, independent contractors and subcontractors shall adhere to and be bound by the terms of this Agreement, including all exhibits.

14.3. Vendor shall be and remain liable for all damages to OST, the Board and the State caused by the negligent performance or non-performance of work under this Agreement by any use temporary staff, independent contractors or a subcontractor.

14.4. The compensation otherwise due to Vendor pursuant to **Exhibit 2** shall not be affected by OST's approval of Vendor's request to use temporary staff, independent contractors or a subcontractor.

15. Complete Agreement.

15.1. This Agreement and its exhibits, which are incorporated herein by reference, shall constitute the entire Agreement between OST and Vendor with respect to the subject matter of this Agreement and shall not be modified or changed without the express written consent of the parties. The provisions of this Agreement supersede all prior oral and written quotations, communications, agreements and understandings of the parties with respect to the subject matter of this Agreement. Notwithstanding the foregoing, or any other provision of this Agreement, all oaths, representations and warranties made by Vendor through participation in the RFP process, including, without limitation, all written representations made by Vendor in Vendor's proposal concerning Vendor's experience and capabilities, shall survive execution and become part of the Agreement.

15.2. If the scope of any provision of this Agreement is too broad in any respect to permit enforcement to its full extent, then such provision shall be enforced to the maximum extent permitted by law, and the parties hereto consent and agree that such scope may be judicially modified accordingly and that the whole of such provisions of the Agreement shall not thereby fail, but the scope of such provision shall be curtailed only to the extent necessary to conform to the law.

15.3. If any term or provision of this Agreement is found by a court of competent jurisdiction to be invalid, illegal or otherwise unenforceable, the same shall not affect the other terms or provisions hereof or the whole of this Agreement, but such term or provision shall be deemed modified to the extent necessary in the court's opinion to render such term or provision enforceable, and the rights and obligations of the parties shall be construed and enforced accordingly, preserving to the fullest permissible extent the intent and agreements of the parties herein set forth.

15.4. Each exhibit to this Agreement, except as its terms otherwise expressly provide, shall be a complete statement of its subject matter and shall supplement, modify and supersede the terms and conditions of this Agreement. No other agreements, representations, warranties or other matters, whether oral or written, shall be deemed to bind the parties hereto with respect to the subject matter of this Agreement.

16. Miscellaneous Provisions.

16.1. Except for fees that may be due and owing as set forth in Section 2 above and **Exhibit 2** hereto, Vendor shall solely bear the costs incurred in the performance of this Agreement.

16.2. Neither this Agreement nor any exhibit may be modified or amended except by the mutual written agreement of the parties. No waiver of any provision of this Agreement shall be effective unless it is in writing and signed by the party against whom enforcement is sought.

16.3. The delay or failure by either party to exercise or enforce any of its rights under this Agreement shall not constitute or be deemed a waiver of that party's right thereafter to enforce

those rights, nor shall any single or partial exercise of any such right preclude any other or further exercise thereof or the exercise of any other right.

16.4. Vendor covenants that it presently has no interest, and that it will not acquire any interest, direct or indirect, that conflicts or would conflict in any manner or degree with the performance of Services required under this Agreement. Vendor further covenants that Vendor has disclosed and adequately described all direct ownerships interests in, or any reseller, consulting or other business relationships with, a Digital Government Services vendor as of the date of this Agreement. Vendor will immediately notify OST of any material changes to such disclosures and descriptions and any other ownership interests in or relationships with a Digital Government Services vendor that arise during the term of the Agreement, including any extension period.

16.5. Vendor acknowledges that OST, the Board and the State have obligations to ensure that public funds and resources are not used to subsidize private discrimination. Vendor recognizes that its refusal to hire or do business with an individual or company due to reasons of race, color, gender, ethnicity, disability, national origin, age, or any other protected status, may result in OST declaring Vendor in breach of the Agreement, terminating the Agreement without liability and/or taking such additional action as may be warranted under the circumstances.

16.6. Vendor warrants that no person or entity has been employed or retained to solicit or secure this Agreement upon an agreement or understanding for a commission, or a percentage, brokerage or contingent fee. For breach or violation of this warranty, OST shall have the right to terminate this Agreement without liability.

16.7. This Agreement was drafted with the joint participation of both parties and shall be construed neither against nor in favor of either party.

16.8. At the option of OST, the parties shall attempt in good faith to resolve any dispute arising out of or relating to this Agreement promptly by negotiation between officials or executives who have authority to settle the controversy. All offers, promises, conduct and statements, in each case relating to dispute resolution, whether oral or written, made in the course of the negotiation by any of the parties, their agents, employees, experts and attorneys are confidential, privileged and inadmissible in any proceeding involving the parties; provided, however, that evidence that is otherwise admissible or discoverable may not be rendered inadmissible merely because it was the subject of discussion in the course of negotiation.

16.9. Any disputes, claims or controversies arising out of or relating to this Agreement that are not resolved through resolution pursuant to Section 16.8, may be submitted to mediation if OST so elects. Any such proceedings held pursuant to this provision shall be governed by the State's laws, and venue shall be in this State. The parties shall maintain the confidential nature of the proceedings and shall keep the terms of any resulting settlement or award confidential to the extent permissible under applicable law. Each party shall bear its own costs of mediation, including attorneys' fees and half of the mediator's fees and expenses.

16.10. The rights and remedies of OST and the State provided for in this Agreement are in addition to any other rights and remedies provided by law or at equity.

16.11. Neither party to this Agreement shall be liable for damages resulting from delayed or defective performance of its obligations under this Agreement when such delays or defective performance arise out of causes beyond the reasonable control and without the negligence or willful misconduct of the party.

16.12. This Agreement, including all exhibits, and its contents, including pricing information, is a public document subject to mandatory disclosure under the State's Freedom of Information Act, 29 *Del. C.* § 10001-10007. In the event that OST is required by law (any statute, governmental rule or regulation, or judicial or governmental order, judgment or decree) to disclose to the public any information or document reasonably designated as "confidential" by Vendor, OST will, to the extent reasonably practicable, give Vendor prior written notice of such disclosure or potential disclosure.

16.13. The provisions of this Agreement are for the sole benefit of the parties hereto. This Agreement confers no rights, benefits or claims upon any person or entity not a party hereto, including any permitted independent contractor or subcontractor approved by OST.

16.14. The terms of the RFP and any addenda or answers to RFP questions (the "RFP Documents") are incorporated herein by reference and govern the Services and Vendor except to the extent the terms of the RFP Documents conflict with the terms of this Agreement. When construing or interpreting the Agreement (a) the terms of the exhibits shall control and take precedence over the main text of the Agreement; and (b) the terms of the Agreement, including all exhibits, shall control and take precedence over the RFP Documents.

17. Assignment of Antitrust Claims.

As consideration for the award and execution of this Agreement by OST, Vendor hereby grants, conveys, sells, assigns and transfers to the State all of Vendor's right, title and interest in and to all known or unknown causes of action it presently has or may now or hereafter acquire under the antitrust laws of the United States or this State relating to the Services and other work product purchased or acquired by OST, the Board or the State pursuant to this Agreement.

18. Governing Law.

This Agreement shall be governed by and construed in accordance with Delaware law, without regard to conflict of laws rules or principles. Vendor consents to jurisdiction and venue in this State.

19. Notices.

Any and all notices required by the provisions of this Agreement shall be in writing and shall be mailed, certified or registered mail, return receipt requested. All notices shall be sent electronically to the following addresses:

If to OST:
Attn:

If to Vendor:
Attn:

IN WITNESS THEREOF, the parties hereto have caused this Agreement to be duly executed as of the date indicated below.

STATE OF DELAWARE, by and through the OFFICE OF THE STATE TREASURER, on behalf of the CASH MANAGEMENT POLICY BOARD

_____
Signature

_____
Name

_____
Title

_____
Date

DEPARTMENT OF TECHNOLOGY AND INFORMATION

_____
Signature

_____
Name

_____
Title

_____
Date

DEPARTMENT OF STATE

_____
Signature

_____
Name

_____
Title

_____
Date

[VENDOR]

_____
Signature

_____
Name

_____
Title

_____
Date

The following exhibits are attached and shall be considered part of this Agreement:

- **Exhibit 1 – Statement of Work**
- **Exhibit 2 – Fee Structure**
- **Exhibit 3 – Cloud Services Terms and Conditions**
- **Exhibit 4 – Data Usage Terms and Conditions**

Exhibit 1: Statement of Work[3]

[To be negotiated.]

[3] Terms used but not defined in the exhibits to this Agreement shall have the meanings ascribed to such terms in the Agreement.

Exhibit 2: Fee Structure

[To be negotiated.]

Exhibit 3: Cloud Services Terms and Conditions

STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd., Dover, Delaware 19904

DELAWARE CLOUD SERVICES TERMS AND CONDITIONS AGREEMENT

PUBLIC AND NON-PUBLIC DATA OWNED BY THE STATE OF DELAWARE

XaaS Contract # _____, Appendix _____

between State of Delaware and _____ dated _____

	Public Data	Non Public Data	Cloud Services (CS) Terms
			PROVIDER must satisfy Clause CS1-A OR Clauses CS1-B and CS1-C, AND Clause CS4 for all engagements involving non-public data. **Clause CS2 is mandatory for all engagements involving non-public data.** **Clause CS3 is only mandatory for SaaS or PaaS engagements involving non-public data.**
CS1-A		✔	**Security Standard Compliance Certifications:** The PROVIDER shall meet, and provide proof of, one or more of the following Security Certifications. • CSA STAR – Cloud Security Alliance – Security, Trust & Assurance Registry (Level Two or higher) • FedRAMP - Federal Risk and Authorization Management Program
CS1-B		✔	**Background Checks:** The PROVIDER must warrant that they will only assign employees and subcontractors who have passed a state-approved criminal background checks. The background checks must demonstrate that staff, including subcontractors, utilized to fulfill the obligations of the contract, have no convictions, pending criminal charges, or civil suits related to any crime of dishonesty. This includes but is not limited to criminal fraud, or any conviction for any felony or misdemeanor offense for which incarceration for a minimum of 1 year is an authorized penalty. The PROVIDER shall promote and maintain an awareness of the importance of securing the State's information among the Service Provider's employees and agents. Failure to obtain and maintain all required criminal history may be deemed a material breach of the contract and grounds for immediate termination and denial of further work with the State of Delaware.
CS1-C		✔	**Sub-contractor Flowdown:** The PROVIDER shall be responsible for ensuring its subcontractors' compliance with the security requirements stated herein.
CS2		✔	**Breach Notification and Recovery:** The PROVIDER must notify the State of Delaware immediately of any incident resulting in the destruction, loss, unauthorized disclosure, or alteration of State of Delaware data. If data is not encrypted (*see* CS3, below), Delaware Code (6 Del. C. §12B-100 et seq.) requires public breach notification of any incident resulting in the loss or unauthorized disclosure of Delawareans' Personally Identifiable Information (PII, as defined in Delaware's *Terms and Conditions Governing Cloud Services* policy) by PROVIDER or its subcontractors. The PROVIDER will provide notification to persons whose information was breached without unreasonable delay but not later than 60 days after determination of the breach, except 1) when a shorter time is required under federal law; 2) when law enforcement requests a delay; 3) reasonable diligence did not identify certain residents, in which case notice will be delivered as soon as practicable. All such communication shall be coordinated with the State of Delaware. Should the PROVIDER or its contractors be liable for the

	Public Data	Non Public Data	Cloud Services (CS) Terms
			PROVIDER must satisfy Clause CS1-A OR Clauses CS1-B and CS1-C, AND Clause CS4 for all engagements involving non-public data. **Clause CS2 is mandatory for all engagements involving non-public data.** **Clause CS3 is only mandatory for SaaS or PaaS engagements involving non-public data.**
			breach, the PROVIDER shall bear all costs associated with investigation, response, and recovery from the breach. This includes, but is not limited to, credit monitoring services with a term of at least three (3) years, mailing costs, website, and toll-free telephone call center services. The State of Delaware shall not agree to any limitation on liability that relieves the PROVIDER or its subcontractors from its own negligence, or to the extent that it creates an obligation on the part of the State to hold a PROVIDER harmless.
CS3		✔	**Data Encryption:** The PROVIDER shall encrypt all non-public data in transit, regardless of transit mechanism. For engagements where the PROVIDER stores Personally Identifiable Information (PII) or other sensitive, confidential information, it shall encrypt this non-public data at rest. The PROVIDER's encryption shall meet validated cryptography standards as specified by the National Institute of Standards and Technology in FIPS140-2 and subsequent security requirements guidelines. The PROVIDER and State of Delaware will negotiate mutually acceptable key location and key management details. Should the PROVIDER not be able to provide encryption at rest, it must maintain cyber security liability insurance coverage for the duration of the contract. Coverage must meet the State of Delaware's standard in accordance with the *Terms and Conditions Governing Cloud Services* policy.
CS4	✔	✔	**Notification of Legal Requests**: The PROVIDER shall contact the State of Delaware upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the State. With regard to State of Delaware data and processes, the PROVIDER shall not respond to subpoenas, service of process, and other legal requests without first notifying the State unless prohibited by law from providing such notice.

The terms of this Agreement shall be incorporated into the aforementioned contract. Any conflict between this Agreement and the aforementioned contract shall be resolved by giving priority to this Agreement. By signing this Agreement, the PROVIDER agrees to abide by the following applicable Terms and Conditions:

FOR OFFICIAL USE ONLY

☐ **CS4 (Public Data)**

☐ **CS1-A and CS4 (Non-Public Data) OR** ☐ **CS1-B and CS1-C and CS4 (Non-Public Data)**

☐ **CS2 (Non-public Data)** ☐ **CS3 (SaaS, PaaS – Non-public Data)**

PROVIDER Name/Address *(print):* _____

_____

_____

PROVIDER Authorizing Official Name *(print):* _____

PROVIDER Authorizing Official Signature: _____ Date: _____

Exhibit 4: Data Usage Terms and Conditions

STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd., Dover, Delaware 19904

DELAWARE DATA USAGE TERMS AND CONDITIONS AGREEMENT

PUBLIC AND NON-PUBLIC DATA OWNED BY THE STATE OF DELAWARE

Contract/Agreement #/name _____, Appendix ___

between State of Delaware and _____ dated _____

	Public Data	Non Public Data		DATA USAGE (DU) TERMS
DU1	√	√	**Data Ownership**	The State of Delaware shall own all right, title and interest in its data that is related to the services provided by this contract. The PROVIDER shall not access State of Delaware user accounts, or State of Delaware data, except (i) in the course of data center operations, (ii) response to service or technical issues, (iii) as required by the express terms of this contract, or (iv) at State of Delaware's written request. All information obtained or generated by the PROVIDER under this contract shall become and remain property of the State of Delaware.
DU2	√	√	**Data Usage**	PROVIDER shall comply with the following conditions. At no time will any information, belonging to or intended for the State of Delaware, be copied, disclosed, or retained by PROVIDER or any party related to PROVIDER for subsequent use in any transaction. The PROVIDER will take reasonable steps to limit the use of, or disclosure of, and requests for, confidential State data to the minimum necessary to accomplish the intended purpose under this agreement. PROVIDER may not use any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service. Protection of Personally Identifiable Information (PII, as defined in the State's *Terms & Conditions Governing Cloud Services* policy), privacy, and sensitive data shall be an integral part of the business activities of the PROVIDER to ensure that there is no inappropriate or unauthorized use of State of Delaware information at any time. The PROVIDER shall safeguard the confidentiality, integrity, and availability of State information. Only duly authorized PROVIDER staff will have access to the State of Delaware data and may be required to obtain security clearance from the State. No party related to the PROVIDER may retain any data for subsequent use in any transaction that has not been expressly authorized by the State of Delaware.

	Public Data	Non Public Data		DATA USAGE (DU) TERMS
DU3	√	√	**Termination and Suspension of Service**	In the event of termination of the contract, the PROVIDER shall implement an orderly return (in CSV or XML or another mutually agreeable format), or shall guarantee secure disposal of State of Delaware data. *Suspension of services:* During any period of suspension or contract negotiation or disputes, the PROVIDER shall not take any action to intentionally alter, erase, or otherwise render inaccessible any State of Delaware data. *Termination of any services or agreement in entirety:* In the event of termination of any services or agreement in entirety, the PROVIDER shall not take any action to intentionally alter, erase, or otherwise render inaccessible any State of Delaware data for a period of 90 days after the effective date of the termination. Within this 90-day timeframe, vendor will continue to secure and back up State of Delaware data covered under the contract. After such 90-day period, the PROVIDER shall have no obligation to maintain or provide any State of Delaware data. Thereafter, unless legally prohibited, the PROVIDER shall dispose securely of all State of Delaware data in its systems or otherwise in its possession or control, as specified herein. Post-Termination Assistance: The State of Delaware 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 Service Level Agreement.
DU4		√	**Data Disposition**	At the end of this engagement, PROVIDER will account for and return all State data in all of its forms, disk, CD / DVD, tape, paper, for example. At no time shall any data or processes that either belong to or are intended for the use of State of Delaware or its officers, agents, or employees, be copied, disclosed, or retained by the PROVIDER. When required by the State of Delaware, the PROVIDER shall destroy all requested data in all of its forms (e.g., disk, CD/DVD, backup tape, paper). Data shall be permanently deleted, and shall not be recoverable, in accordance with National Institute of Standards and Technology (NIST) approved methods. The PROVIDER shall provide written certificates of destruction to the State of Delaware.
DU5		√	**Data Location**	The PROVIDER shall not store, process, or transfer any non-public State of Delaware data outside of the United States, including for back-up and disaster recovery purposes. The PROVIDER will permit its personnel and subcontractors to access State of Delaware data remotely only as required to provide technical or call center support.

	Public Data	Non Public Data		DATA USAGE (DU) TERMS
DU6		**√**	**Breach Notification and Recovery**	The PROVIDER must notify the State of Delaware immediately of any incident resulting in the destruction, loss, unauthorized disclosure, or alteration of State of Delaware data. If data is not encrypted (*see* DU7, below), Delaware Code (6 Del. C. §12B-100 et seq.) requires public breach notification of any incident resulting in the loss or unauthorized disclosure of Delawareans' Personally Identifiable Information (PII, as defined in Delaware's *Terms and Conditions Governing Cloud Services* policy) by PROVIDER or its subcontractors. The PROVIDER will provide notification to persons whose information was breached without unreasonable delay but not later than 60 days after determination of the breach, except 1) when a shorter time is required under federal law; 2) when law enforcement requests a delay; 3) reasonable diligence did not identify certain residents, in which case notice will be delivered as soon as practicable. All such communication shall be coordinated with the State of Delaware. Should the PROVIDER or its contractors be liable for the breach, the PROVIDER shall bear all costs associated with investigation, response, and recovery from the breach. This includes, but is not limited to, credit monitoring services with a term of at least three (3) years, mailing costs, website, and toll-free telephone call center services. The State of Delaware shall not agree to any limitation on liability that relieves the PROVIDER or its subcontractors from its own negligence, or to the extent that it creates an obligation on the part of the State to hold a PROVIDER harmless.
DU7		**√**	**Data Encryption**	The PROVIDER shall encrypt all non-public data in transit, regardless of transit mechanism. For engagements where the PROVIDER stores Personally Identifiable Information (PII) or other sensitive, confidential information, it shall encrypt this non-public data at rest. The PROVIDER's encryption shall meet validated cryptography standards as specified by the National Institute of Standards and Technology in FIPS140-2 and subsequent security requirements guidelines. The PROVIDER and State of Delaware will negotiate mutually acceptable key location and key management details. Should the PROVIDER not be able to provide encryption at rest, it must maintain cyber security liability insurance coverage for the duration of the contract. Coverage must meet the State of Delaware's standard in accordance with the *Terms and Conditions Governing Cloud Services* policy.

The terms of this Agreement shall be incorporated into the aforementioned contract. Any conflict between this Agreement and the aforementioned contract shall be resolved by giving priority to this Agreement. By signing this Agreement, the PROVIDER agrees to abide by the following applicable Terms and Conditions [check one]:

FOR OFFICIAL USE ONLY ☐ **DU 1 - DU 3 (Public Data Only) OR** ☐ **DU 1 - DU 7 (Non-public Data)**

PROVIDER Name/Address *(print):* _____

_____

PROVIDER Authorizing Official Name *(print):* _____

PROVIDER Authorizing Official Signature: _____ Date: _____

APPENDIX B: SCOPE OF SERVICES

Vendors shall submit a detailed scope of work outlining proposals to the State, for one or more of the following components:

I. WEB AND APPLICATION DESIGN

The State is seeking an itemized proposal with corresponding pricing for web and application design services that shall result in a centralized web and mobile user interface tied to the gateway and merchant processing products and services components outlined in the proceeding Scope of Services sections outlined below. The central tenet for web and application design services is flexibility, wherein the State envisions various interaction capabilities depending upon the needs and capabilities of existing applications. Solution will be designed to support future products and services components beyond merchant processing. Web and application design services shall include the sharing of information via the State's web and mobile portal with all customers through a variety of multi-media formats, including text, graphics and video; transaction processing between the State and its customers over the internet, credit card processing, application development, integration with customers' existing systems, security, application hosting & support.

The continued delivery of existing Digital Government services and information resources and the development of new and improved Digital Government services are of paramount importance. It is anticipated that the electronic delivery of government services will continue to facilitate and improve the way Customers communicate and interact with government. The table below describes possible integration capabilities. Agency applications and websites shall have the flexibility to integrate with a centralized web and mobile user interface that includes one or more of the following capabilities to be described in the Vendor(s) submission:

Integration Capabilities	**Functionality**
Basic	The centralized web and mobile user interface provide basic information about the website or application including URLs, summary data, responsible agency, and other metadata that help users identify whether the website or application may be relevant to their needs and interests. Core Design Principles: • Sign in once for any government service, • Fast and secure one-click stored payments,

	• Predictive approach anticipating citizen needs, • Evolving profiles based on user behavior and data analysis, • Profile, preferences & activity data driving content results, and • Available seamlessly on any device.
Commerce	The centralized web and mobile user interface provide payment services for the website or application outlined in the corresponding gateway and merchant processing sections of the Scope of Services below.
Application Enhancement and Augmentation	The centralized web and mobile user interface shall provide some level of application functionality on behalf of the website or application. This may include providing application forms or other capabilities directly within the platform that are then transmitted back to the agency application or database upon completion and submission by a user (e.g. applications for State services).
Master Data Management	The centralized web and mobile user interface shall provide real-time information to users concerning upcoming deadlines, opportunities, and related information that are relevant to the user on behalf of the agency website or application. Applications that integrate at this level will expose information through the platform that will help users identify and track information about their relationship with the State of Delaware. Examples of information that the platform could provide to end users that is associated with applications that integrate at this tier are as follows: 1. "Did you know that your fishing license needs to be renewed in 30 days? Click here for more information" 2. "You registered a new business. Here are other filing requirements that may be applicable to your new firm."

3. "Many teachers also participate in these volunteer opportunities. Click here for more information."

Additional specifications outlined in a Vendor's proposal shall include:

a. An outline of all components listed above included the capabilities for search functionality, directory management, the transmission and receipt of RSS feeds;
b. A description of managed hosting infrastructure (e.g. hardware, operating systems, network, communications, connectivity, backup, fail-over, disaster recovery components, etc.);
c. Assurance that SAAS Solutions maintain an independent Tenant for the State's service;
d. Evidence of IPS signatures and events being maintained, which may be requested by the state for validation;
e. A description of managed hosting services (e.g. software and hardware installation, updating, patch application, monitoring, tuning, disaster recovery and backup support, emergency and planned network, system, application maintenance, etc.);
f. Assurance that credentials stored in middleware solutions are encrypted at rest or in configuration files;
g. A fully patched operating system with 3rd applications included in patch assessment and patch application;
h. A description of active services such as web services and hardening standards;
i. A comprehensive next generation endpoint security solution with machine learning capable anti-malware, abnormally detection, file integrity monitoring, log file monitoring, host-based intrusion detection, and file reputation scanning;
j. Host based disk encryption;
k. Auditing on hosts capturing all security related activities and the environment must maintain the event logs for up to 7 years;
l. Access to application data noted as restricted to only authorized database administrators;
m. Application authentication supporting federation with state or agency identity stores to ensure governance over access and the certification of access;
n. Potential integration with the State's Identity management (IAM) solution (OKTA);
o. Support new user identity proofing; government ID and Knowledge-based validation during registration; directly or through the State's IAM solution;
p. Include user authentication to the system;
q. Support for OpenID Connect, OAuth and or SAML;
r. Internet Facing web front-end servers must be protected with an enterprise web application firewall with protections to include the OWASP Top 10, Botnets, DDoS and application virtual patching;
s. Applications requiring the use of the state's brand and domain name to traverse cloud-based Web Application Firewall for centralized visibility to all brand threats;
t. Assurance that application communications from users and across components of the application are encrypted;
u. Application security related events like logins, changes and administrator activities are logged and reviewed for malicious or abnormal activity;

v. That applications must undergo application code scans at least yearly and before any changes are loaded into production;
w. That applications must undergo dynamic application scans at least yearly and after any changes are loaded into production;
x. Notification to the System Administrator regarding which releases of third-party software are known to create problems with the current version of the vendor software within 24 hours of the update announcement;
y. A description of your approach to installation and configuration of all software, hardware, and cloud services necessary to provide a complete working environment to meet the initial performance requirements of the centralized web and mobile user interface, integration with State of Delaware Master Data Management , and integration with Customer Agency applications. Additionally, to the extent that cloud computing is used in your solution, explain how your solution will utilize, configure, maintain, and update cloud computing resources;
z. A description of your approach to providing post deployment ongoing support, maintenance, and upgrades;
aa. A description of your approach to day-to-day operations, maintenance, and administration of the centralized web and mobile user interface. The platform shall operate 24 hours per day every day of the year. Operations include customer service, facilities, hardware, networking, security, performance monitoring, and problem resolution. Maintenance includes keeping all off-the-shelf software on current releases and keeping the development environment on mainstream industry and State accepted standards. Administration includes all financial, record keeping, reporting, and management aspects of the platform;
bb. An example of integration scenarios that explain the process, methodology, and technology solutions associated with the integration of Customer Agency applications with the centralized web and mobile user interface;
cc. Conformity to State Web Presentation Guidelines: https://gic.delaware.gov/web-standards/ and the specific editions of the standards and guidelines listed in Chapter 7 of the Section 508 Standards, especially ISO/IEC 40500:2012, the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0 (https://www.w3.org/TR/WCAG20/);
dd. A description of the usability and compatibility of your solution across internet browsers, devices, and assistive technologies, including desktop and mobile devices supporting all major operating systems, and all major browsers including current and recent versions of Internet Explorer, Google Chrome, Microsoft Edge, Mozilla Firefox, and Safari. Include any applicable VPAT or similar assessments of accessibility of existing technologies and plans to verify usability of solutions while in development and once ready for deployment;
ee. A description of any Third Party certificates of audit certifying on a recurring basis that the centralized web and mobile user interface will comply with, including but not limited to any of the following:
    - NIST 800-53;
    - CSA STAR – Cloud Security Alliance – Security, Trust & Assurance Registry

- Federal Risk and Authorization Management Program (FedRAMP) certification for a System hosted in a cloud environment;
- PCI DSS Compliance;
- Health and Human Services Health Insurance Portability and Accountability Act (HIPAA) Compliance;
- Internal Revenue Service Publication 1075 Compliance; and

ff. A description of the proposed solution's technical and data architecture. Responses should include: how the proposed architecture flexibility adapts, integrates, and utilizes evolving policies, best practices, and operating procedures; utilizes open architecture standards; supports for a distributed computing environment; provides secure data exchange; includes request/reply, publish/subscribe, and synchronous/asynchronous functionality to facilitate information sharing.

II. PAYMENT GATEWAY PRODUCTS AND SERVICES

The State is seeking an itemized proposal with corresponding pricing for point of sale chip reader terminals, virtual terminals, mobile payment, telephone, mail, interactive voice response ("IVR") systems, self-service terminals, electronic cash registers, kiosks, as well as any other internet or electronic payment capture systems offered by the Vendors. Additional specifications outlined in a Vendor's proposal shall include:

a. Hardware terminals for in-person and Mail Order/Telephone Order (MOTO) transactions. This must include credit, PIN debit, and chip reader capabilities;
b. Hosted payment processing options for internet and mobile transactions;
c. Application Program Interface (API) payment processing for integration with State applications, including in-person, internet, mobile and MOTO transactions for all card types;
d. For all solutions, Vendors shall provide detail on whether the devices are PCI validated, including Point to Point Encrypted (P2PE) solutions, as well as NACHA compliant, where applicable;
e. A description of the processes for converting existing solutions and requirements from an existing provider to the Vendors proposed solution(s);
f. A description of the processes for setting up new solutions upon Agency requests, including average turnaround time to set up new gateway solutions;
g. A description of the usability and compatibility of your solution across internet browsers, devices, and assistive technologies, including desktop and mobile devices supporting all major operating systems, and all major browsers including current and recent versions of Internet Explorer, Google Chrome, Microsoft Edge, Mozilla Firefox, and Safari. Include any applicable VPAT or similar assessments of accessibility of existing technologies and plans to verify usability of solutions while in development and once ready for deployment;
h. The mechanism(s) and system(s) to enable State agencies to accept and process merchant transactions and then settle the transactions at a designated financial institution including verification of acceptance of the following payment types:

- Visa;
- MasterCard;
- Discover;
- American Express;
- Debit Cards – Pin and Pin-less;
- Prepaid Cards;
- e-Checks/check verification services, and ACH;
- Ability to add cards in the future, if the need arises;
- Alternate payments to include mobile payment solutions such as Paypal, Venmo, Zelle, Google Pay, Apple Pay, Samsung Pay, customer payment portals and compatible Apps; and
- Emerging payment platforms including Real Time Payments.

i. Daily deposit activity reporting including the transaction date, deposit totals by MID, and total consolidated deposit by batch and/ or State Agency;
j. Summary deposit reporting including total daily deposit by merchant number and total for all depositing agencies, as well as consolidated grand totals of deposits for the month by merchant number and in the aggregate;
k. Detailed transaction activity by MID, batch, or State agency upon request;
l. The capability to separate monthly invoicing for each State Agency with details of monthly activity by MID;
m. The capability for consolidated summary reports sorted by State Agency, as well as access permitted by individual merchants. Include details on the reporting capabilities provided with this system;
n. Applications that will provide credit card information (credit card number, expiration date, charge amount), process the request and return the authorization number to the application. In addition, applications shall identify any variations or additional data elements required. Describe the justification for any additional requirements. Last, applications shall identify and return as raw data any State Agency-created code contained within VAR or VAN industry standard market data;
o. A detailed list of all VAR proprietary software on which it is certified. Include a detailed description with respect to the use of those software systems;
p. Assurance that each transaction will have a unique identifier per location/site for reconciliation, auditing and security purposes;
q. Validation that PC based systems shall, at a minimum, provide the following:

- Operate in a Windows environment;
- Offer a user-friendly package with on-line assistance;
- Provide for open architecture to easily connect to other systems;
- Provide spreadsheet or acceptable alternative formatting for reports;
- Include report view and printing functions;
- Meet the most current PCI DSS Compliance and NACHA Standards;
- Allow for user creation of passwords.

r. A description the operating system and other technical specifications pertinent to any recommended solution(s);
s. The capability for Delaware Agencies to develop proprietary data formats/reporting for credit card authorization and settlement through the use of mechanisms and systems identified in section (i.) above;
t. Applications that provide functional credit card information (credit card number, expiration date, charge amount) that will process the request and return the authorization number to the application;
u. The requirement to add the Remittance ID field to the data and pass same back to agencies to enable reconciliation on this unique field between the business system and the credit card system. The Vendors shall disclose the remittance ID field to each agency per location/site;
v. All replacement and warranty policies for all equipment, including equipment for lease, purchase, or rental;
w. Fraud verification services as listed below but not limited to:

- Address Verification Service, Street Number, Zip Code;
- Card Security Verification Service;
- Real-time authorizations;
- Capabilities to request audit reports based on State Agency specified frequencies or criteria;
- Real or near-real-time analytics of card usage for potential fraud patterns – surveillance utilization review system functionality; and
- Supported by virtual or in-person training.

x. Customer technical support available via a toll-free number twenty-four hours a day, seven days a week, and three hundred sixty-five days per year;
y. Outline their processes for handling chargebacks and adjustments, and include the following specifications:

- Adjustments or chargebacks shall be identified by merchant number and transaction identifier;
- State Agencies shall receive notification of all chargebacks and adjustments;
- Chargebacks and adjustments shall post to the demand deposit account at the financial institution to which it originally settled;
- Chargebacks shall post to the account individually and cannot be combined. Chargebacks must be set up per location to remain separate;
- Describe your process for customer service support with respect to chargebacks;
- Chargebacks/adjustments shall not be netted against daily transmissions/uploads from agencies; and
- Explain in detail how ACH returns are handled.

z. Transactions posting at levels according to each State Agency and within the most current PCI/DSS compliance and NACHA standards, including:
    - Individual merchant number;

- Batch level, or a proposed model for non-batch (real-time) posting; and
- Total or consolidated transactions.

aa. A secure environment for the testing of new applications that is entirely separate from the production environment. Test cards, in sufficient number, shall be provided to agencies performing tests. State employees shall be prohibited in using their own cards for testing purposes;
bb. Safeguards to stop users from accidentally initiating multiple payments in error. Upon award, the Vendors will be expected to supply API documentation;
cc. A notification process to the merchant and OST when any merchant ID has experienced 60 consecutive days without any transaction activity;
dd. The merchant settlement processing timeframe, including whether the Vendors provide daily automatic settlement with an explanation for any next day processing;
ee. Any limitations on files. e.g., number each day, records in a batch, transaction amount, or volume per day;
ff. An explanation of how seasonal MIDs are handled, including activation and de-activations processes;
gg. A description of the authorization and settlement of transactions through the appropriate authorization and settlement networks; and
hh. The back-up procedures in case of system failure to meet availability and respond to time requirements.

III. MERCHANT PROCESSING SERVICES

The State is seeking merchant processing services with connectivity to the State's incumbent gateway services provider, Govolution, as well as any other gateway services and products Vendors that meet the qualifications outlined in Section II of the Scope of Work above. Merchant processing services include transaction processing for all credit, pin debit, prepaid non-pin debit, electronic benefits transfer, ACH, electronic, and other agreed upon payment methods. Additional specifications outlined in a Vendor's proposal shall include:

a. A description and pricing on all data encryption and tokenization services that are not otherwise a service of the gateway services and product provider;
b. The ability to pass the MID within the NACHA 6-7 field for each ACH transaction to the demand deposit account at the designated financial institution in order to correctly post to the State's general ledger;
c. The ability to provide the agency location name associated with each MID in the NACHA 6-8 field for each ACH transaction to the demand deposit account at the designated financial institution;
d. Procedures to establish new merchant accounts on a continuous basis and procedures to review merchant assignments to the pricing schedule on a quarterly basis. Vendors shall receive and make appropriate adjustments for new participants when assessed incorrectly and as requested;
e. A description of the Vendors approaches to facilitating PCI/DSS and NACHA compliance between the State's merchants, card brands and industry associations;

f. A description of the process for settlement each business day to the financial institution and collateralized account(s) designated by OST and approved by the Board. All settlement times will be calculated on Eastern Standard Time;
g. A process to provide updated interchange fee schedules to OST as they are produced by the card brands, the assessment of interchange and other agreed upon transaction fees on a collective or individualized basis with State agencies;
h. Reporting capabilities that include a chargeback activity report organized by MID upon occurrence, the number and dollar amount of chargebacks, and a monthly chargeback activity report organized by MID and location of each agency's activity;
i. The prohibition for individual State agencies to open merchant services accounts directly with the Vendors. All accounts shall be established through OST, and any changes to designated financial institutions for existing accounts must be pre-approved by OST prior to set up; and
j. Assurance that customer technical support is available via a toll-free number twenty-four hours a day, seven days a week, and three hundred sixty-five days per year.

IV. ACCOUNT RECONCILIATION AND FEE ANALYSIS PRODUCTS

The State is seeking account reconciliation and fee analysis software with compatibility to any proposed web and application design, gateway and merchant processing services proposed under the RFP. Account reconciliation software shall be capable of conducting automated account reconciliation and fee analysis software shall be capable of financial statement analysis for the State, OST and State Agencies. Additional specifications outlined in a Vendor's proposal shall include:

a. Account reconciliation software shall possess the capacity to import and export standard and customized data from various sources, including the State's accounting system (First State Financials, Oracle PeopleSoft), automate matching, and journals/exceptions with email notification for any exceptions found. The software shall also provide for standardized reconciliation templates, account certifications, customized reports, process management and monitoring;
b. Account reconciliation software shall possess the capacity for reconciling accounts receivables and payables between the State's general ledger, OST receivables and payables files, and various banking providers;
c. Account reconciliation software shall possess the capacity for reconciling debit, credit, ACH, and other payment methods between the State's general ledger, point of sale files, the merchant processor and various banking providers;
d. Account reconciliation software shall possess the capacity for archiving and retrieval of historical files;
e. Account reconciliation software shall possess the capacity for manual matching, ability to identify duplicate transactions prior to importing a file and for the tracking of transactions that do not match or reconcile;

f. Account reconciliation software shall possess the capacity to create customized reports and dashboards;
g. Fee analysis software shall possess the capability to import transactional data and bank fee statements in a standardized format;
h. Fee analysis software shall be capable of:
    - Flagging bank errors, tracking refunds and credits, and providing audit trails;
    - Analyzing merchant fees including interchange rates and fees, as well as other fees assessed by merchant processors;
    - Capturing and tracking individual account information for multiple accounts such as current signers, addresses, individual account names, contact information, and other customized dashboards;
    - Capturing dormant, overdrawn, underutilized or service-ridden accounts, and performing "what-if" analyses;
    - Importing non-standard statements and making side-by-side comparisons;
    - Creating configurable comparison codes; and
    - Automatically allocating expenses and posting charges to the general ledger.
i. Detailed technical specifications on any software proposed, including:
    - Whether applications are locally (database) hosted, or cloud based (whether via application or web). For cloud-based solutions, specify tenancy, application security protocol, and data storage as detailed in Appendix C;
    - Minimum operating system requirements;
    - Minimum requirements for plug ins, display resolution, web browser compatibility (if applicable), processing and memory;
    - Account reconciliation software shall be compatible with current industry standards such as NACHA, BAI, .txt, and .csv formats;
    - Fee analysis software shall be compatible with current industry standards such as 822, .txt, and .csv formats.

V. ANCILLARY SERVICES:

If and as requested the State, assist with and undertake such other matters as may be reasonably requested.