Stacy Garrity, Pennsylvania Treasurer

REQUEST FOR PROPOSALS FOR

Colocation Data Center Facility

ISSUING OFFICE

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

RFP25-002

DATE OF ISSUANCE

May 9, 2025

TABLE OF CONTENTS

CALENDAR OF EVENTS

The Pennsylvania Treasury Department intends to follow the following schedule. Modifications may become necessary, however, as the activities described in the schedule take place. Treasury will take reasonable steps to inform interested parties of such modifications, including posting them on the Treasury Website.

ACTIVITY	RESPONSIBILITY	DATE
Please monitor the Treasury Procurement website: https://patreasury.gov/procurement for all communications regarding this RFP	Potential Offerors Issuing Office	
Issuance of RFP25-002 (posted to website https://patreasury.gov/procurement)	Issuing Office	May 9, 2025
Deadline for potential Offerors to submit clarification questions via email to the RFP mailbox: RFP25-002@patreasury.gov	Potential Offerors	May 15, 2025
Answers to potential Offerors' questions submitted by the deadline will be posted to the website. https://patreasury.gov/procurement	Issuing Office	May 28, 2025
Proposals must be received by the Issuing Office by 5PM EST. Proposals are accepted only via email to RFP25-002@patreasury.gov	Potential Offerors	June 9, 2025
Proposal Presentations (optional)	Potential Offerors	Week of June 30, 2025
Treasury requests for clarification sent to Offerors	Issuing Office	July 9, 2025
Responses to request for clarification must be received by the Issuing Office by 5PM EST via email to RFP25-002@patreasury.gov	Potential Offerors	July 16, 2025
On-site visits (optional): Treasury RFP committee to Offerors	Issuing Office/ Potential Offerors	Week of July 21, 2025
Best-and-Final Offer letters sent (optional)	Issuing Office	Aug 7, 2025
Responses to Best-and-Final Offer must be received by Issuing Office by 5PM EST via email to RFP25-002@patreasury.gov	Potential Offerors	Aug 14, 2025

PART I: GENERAL INFORMATION

I-1. Purpose

Pennsylvania Treasury Department ("Treasury") is seeking proposals from qualified offerors to provide reliable colocation data center facility and related services. These services are essential to Treasury's ability to operate seamlessly if/when disaster strikes the primary data center location in Harrisburg, Pennsylvania.

This request for proposal ("RFP") provides sufficient information to enable those interested ("Offerors") to prepare and submit proposals for Treasury's consideration, on behalf of the Commonwealth of Pennsylvania ("Commonwealth"), to provide reliable colocation data center facility and related services.

I-2. Problem Statement

Treasury is an independent administrative agency of the Commonwealth of Pennsylvania and is responsible for disbursement of funds by the Commonwealth, as well as the deposit, investment, and safekeeping of money and securities belonging to the Commonwealth. The State Treasurer is the head of Treasury and the statutory custodian of the funds of most state agencies, which totaled approximately $170 billion. As part of Treasury's statutory responsibilities as custodian, from July 2023 through June 2024, the Department processed over 18.9 million payments and expenditures totaling over $128.1 billion, an average of 2.7 disbursements every second of every day. These payments include but are not limited to: Long-term care benefits for nursing homes; approximately 390,000 monthly pension payments; payments for health insurance providers for elderly and the disabled; benefit payments; and vendor payments and data transfer. Further, Treasury is considered the bank for the Commonwealth and needs to have communication with outside financial institutions as well as the agencies of the Commonwealth of Pennsylvania.

These are just some of Treasury's critical functions that require a reliable disaster recovery data center that has multiple backup systems. Therefore, PA Treasury desires to select a vendor to provide reliable colocation data center facility and related services, commencing no later than March 1, 2026, to avoid any interruption in the delivery of these essential services to Pennsylvania residents.

I-3. Issuing Office

Treasury ("Issuing Office") has issued this RFP on behalf of the Commonwealth. The sole point of contact in the Commonwealth for this RFP shall be Treasury's Issuing Office via email to RFP25-002@patreasury.gov.

I-4. Scope

This RFP contains instructions governing the requested proposals, including the requirements for the information and material to be included; a description of the services to be provided; mandatory requirements which Offerors must meet to be eligible for consideration; requirements and qualifications for general evaluation criteria; and other requirements specific to this RFP.

I-5. Type of Contract

Except as described in more detail elsewhere in this RFP, the Issuing Office desires to enter a Contract containing Treasury's Standard Contract Terms and Conditions as referenced in **Appendix A** of this RFP.

The Issuing Office, in its sole discretion, may undertake negotiations with Offerors whose proposals, in the judgment of the Issuing Office, show them to be qualified, responsible and capable of performing the work.

I-6. Rejection of Proposals

The Issuing Office reserves the right, in its sole and complete discretion, to reject any proposal received because of this RFP. Treasury reserves the right to accept or reject and to waive any informalities or irregularities in the proposals and to contract as the best interests of Treasury require to obtain the services described in this RFP. Selection of an Offeror's proposal does not mean that all aspects of the proposal are acceptable to Treasury. Treasury reserves the right to negotiate terms and conditions with the selected Offeror before executing the contract.

I-7. Incurring Costs

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

I-8. Proposal Presentations

The Issuing Office will hold a Proposal Presentation as specified in the Calendar of Events. The purpose of the presentations is to provide an opportunity for clarification of the technical submittals. Attendance at the Proposal Presentation, which will be conducted virtually, is mandatory as it will affect scoring. Additional information regarding scheduling of the Proposal Presentations will be sent from the Issuing Office via email from RFP25-002@patreasury.gov to responsive Offerors.

I-9. Questions and Answers

Any questions related to this RFP must be submitted by email (with the subject line "RFP25-002 Questions") to the Issuing Office via email to RFP25-002@patreasury.gov . Questions must be submitted by the Offeror and received by the Issuing Office no later than the dates and times indicated on the Calendar of Events. The Offeror shall not attempt to contact the Issuing Office by any other means.

The Issuing Office shall post all questions (including questions relating to cost submissions), and their answers, on the Treasury's Procurement Website https://patreasury.gov/procurement/, as well as send to all Offerors via email from RFP25-002@patreasury.gov.

The Issuing Office reserves the right to answer questions filed after the last deadline if it determines that responding will clarify or correct a previously undetected ambiguity or error or otherwise allows all Offerors the ability to provide better proposals, thereby advancing the interests of the Commonwealth.

All questions and responses as posted on the Treasury website are considered as addenda to, and part of, this RFP in accordance with **Part I, Section I-10**. Each Offeror is responsible for monitoring the Treasury website for new or revised RFP information. The Issuing Office shall not be bound by any oral information communicated to or by it, and it shall not be bound by any written information that is not either contained within the RFP or formally issued as an addendum by the Issuing Office. The Issuing Office does not consider questions to be a protest of the specifications or the solicitation.

I-10. Addenda to the RFP

If the Issuing Office deems it necessary to revise any part of this RFP before the proposal response date, the Issuing Office will post an addendum to that effect to Treasury's Procurement Website https://patreasury.gov/procurement/. It is the Offeror's responsibility to periodically check the website for any new information or addenda to the RFP. As previously noted, answers to the questions submitted will be posted to the website as addenda to the RFP.

I-11. Response Date and Time

To be considered for selection, proposals must arrive in the Issuing Office mailbox RFP25-002@patreasury.gov on or before the date specified in the RFP Calendar of Events. Proposals must be submitted no later than 5PM EST.

Please request a delivery receipt as proof of the time of submission. The Issuing Office **will not** accept proposals via facsimile transmission. In the event of an extension of the response date, the time (hour) for submission of proposals shall remain the same. The Issuing Office will reject any late proposals.

I-12. Proposal Format and Submission

Format

Offerors shall submit proposals via email to RFP25-002@patreasury.gov in Adobe PDF, Microsoft Office (.docx and .xlsx file formats), or Microsoft Office-compatible format, utilizing navigation headings (Microsoft Word) or bookmarks (Adobe) that match the sections given in **Part II**. Each page must be numbered for ease of reference. Any spreadsheets must be in Microsoft Excel, with no protection applied to the workbook or any sheet within.

How to Submit

An official authorized to bind the Offeror to its provisions must sign the proposal. If the official signs the Proposal Cover Sheet (**Appendix D** to this RFP) and the Proposal Cover Sheet is attached to the Offeror's proposal, the requirement will be met.

The proposal must contain each of the following submittal sections in a **separate email** with the following subject lines and contents:

A. Technical Submittal

Email subject: Technical Submittal [Vendor Name] RFP25-002
Contents: Copy of Proposal Cover Sheet
Technical Submittal
The Offeror must ensure no cost information is included in Technical Submittal.

B. Small Diverse Business Submittal

Email subject: SDB Submittal [Vendor Name] RFP25-002
Contents: Copy of Proposal Cover Sheet
Small Diverse Business Submittal
The Offeror must ensure no cost information is included in SDB Submittal.

C. Cost Submittal

Email subject: Cost Submittal [Vendor Name] RFP25-002
Contents: Copy of Proposal Cover Sheet
Cost Submittal
Offeror must include Cost Proposal Sheet

The Offeror shall make no other distribution of its proposal to any other Offerors, Treasury officials, other Treasury public email addresses, Commonwealth officials, or Commonwealth consultants.

The Issuing Office reserves the right to request additional information that, in the Issuing Office's opinion, is necessary to assure that the Offeror's competence, number of qualified employees, business organization, and financial resources are adequate to perform according to the RFP requirements.

The Issuing Office may make inquiries as it deems necessary to determine the ability of the Offeror to perform the requested services. The Offeror shall furnish the Issuing Office with all pertinent information and data, including site visits and requests for additional information. The Issuing Office reserves the right to reject any proposal if the information submitted by such Offeror fails to satisfy the Issuing Office that such Offeror is properly qualified to carry out the obligations of the RFP and to complete the project as specified in this RFP.

The specific contents of the Submittals A-C listed above are further outlined in Section II. In addition to these requirements, the following applies to all proposals:

- The proposal for this RFP must state that it will remain valid for 150 days from the date that an Offeror is selected for negotiation or until a contract is fully executed, whichever is earlier.

- Each Offeror submitting a proposal specifically waives any right to withdraw or modify it, except that the Offeror may withdraw its proposal by notifying the Issuing Office via email at RFP25-002@patreasury.gov prior to the exact hour and date specified for proposal receipt.

- An Offeror may modify its submitted proposal prior to the exact time (hour) and date set for proposal receipt only by submitting via email a new proposal or modification that complies with the RFP requirements and that explicitly requests the Issuing Office to disregard and remove from consideration any prior submitted proposals.

I-13. Proposal Contents

A. Confidential Information.

Treasury is requesting certain information pertaining to security that may be exempt from public disclosure pursuant to Section 67.708 of the Pennsylvania Right-To-Know Law. Offerors are directed to follow Paragraph C and submit a redacted and unredacted proposal. Offeror who determines that it must divulge such information as part of its proposal must submit a signed written statement and must additionally provide a redacted version of its proposal, which removes only the confidential proprietary information and trade secrets, for required public disclosure purposes. A signed written statement must state:

1. The attached document contains confidential or proprietary information or trade secrets under Pennsylvania law and cite the law;
2. The redactions are in accordance with Pennsylvania RTKL 65 P.S. 67.101 et seq.

B. Treasury Use

All material submitted with the proposal, and any work products developed as an outcome of the Contract from this RFP, shall be considered the property of Treasury. Treasury has the right to use any or all ideas not protected by intellectual property rights that are presented in any proposal regardless of whether the proposal becomes part of a Contract. Notwithstanding any Offeror copyright designations contained on proposals, Treasury shall have the right to make copies and distribute proposals internally and to comply with public record or other disclosure requirements under the provisions of any Commonwealth or United States statute or regulation, or rule or order of any court of competent jurisdiction.

C. Public Disclosure

RFP responses are subject to being requested pursuant to Pennsylvania's Right-to-Know Law ("RTKL") (65 P.S. 67.101 et seq.) and may be incorporated into the contract. Except as otherwise noted, Treasury recognizes RFP responses to be public records and will produce them at the appropriate time if requested to disclose under RTKL. If an Offeror wishes to redact any part of its RFP response from disclosure under RTKL, it must submit (in addition to the unredacted proposals required to be submitted by **Part I, Section I-12**) a complete and identical proposal except for those provisions it chooses to redact in PDF format via email to RFP25-002@patreasury.gov. Redacted RFP responses must be appropriately labeled to enable them to be readily distinguished from unredacted responses. All redactions must be in accordance with the exceptions set forth in RTKL and must be detailed to Treasury in an accompanying letter. Treasury will not provide legal advice on RTKL or redactions to any Offerors. If an Offeror does not submit a redacted response, Treasury will treat the entire RFP response as a public record under RTKL and will provide it to requesters as such.

I-14. Other Communications and Submissions

All communications between Offerors and Treasury shall be sent to, and will originate from, the email address RFP25-002@patreasury.gov, including the complete response to this RFP as described in **Part I, Section I-12**. Except as otherwise indicated in the Calendar of Events, all responses must be submitted no later than 5:00PM EST.

I-15. Small Diverse Business Information

The Issuing Office is continually exploring new ways to encourage participation by small diverse businesses as prime contractors and encourages all prime contractors to make significant strides to use small diverse businesses as subcontractors and suppliers. Treasury acknowledges and supports the Department of General Services (DGS) self-certification process found on the DGS website https://www.dgs.pa.gov/Small%20Diverse%20Business%20Program/Pages/Process.aspx

The Small Diverse Business (SDB) Program and Veteran Business Enterprise (VBE) Program encourage and ensure open and equitable contracting practices are used by prime contractors in soliciting and

contracting with small diverse and veteran-owned businesses during the Request for Proposal (RFP) procurement process.

See Part II for additional information.

I-16. Economy of Preparation

Offerors should prepare proposals simply and economically, providing a straightforward, concise description of the Offeror's ability to meet the requirements of the RFP.

I-17. Clarification on Responses

Offerors are required to provide clarification of their proposals to the Issuing Office to ensure thorough mutual understanding and Offeror responsiveness to the solicitation requirements. The Issuing Office will initiate requests for clarification. Clarifications may be sought from Offerors at any stage of the evaluation and selection process prior to Contract execution.

I-18. Prime Contractor Responsibilities.

The Contract will require the Offeror to assume responsibility for all services offered in its proposal whether it produces them itself or by subcontract. The Issuing Office will consider the Offeror to be the sole point of contact with regards to contractual matters.

I-19. Best-and-Final Offers

A. While not required, the Issuing Office reserves the right, in its sole discretion, to conduct discussions with Offerors for the purpose of obtaining best-and-final offers. To obtain best-and-final offers from Offerors, the Issuing Office may do one or more of the following, in any combination and order:

i. Schedule oral presentations
ii. Request revised proposals

B. Even in an instance where the Issuing Office elects to solicit best-and-final offers, the following Offerors will not be invited by the Issuing Office to submit a best-and-final offer:

i. Those Offerors that the Issuing Office has determined to be not responsible or whose proposals the Issuing Office has determined to be not responsive.
   a. "**Responsible**" shall mean the Offeror possesses the experience, facilities, reputation, financial resources and are fully capable of performing the contract.
   b. "**Responsive**" shall mean the proposal response complies, without material deviation, with the requirements of the solicitation, including the Technical Submittal and attached appendices.
ii. Those Offerors that the Issuing Office has determined, from the submitted and other information, do not possess the experience or qualifications to assure good faith performance of the Contract.
iii. The Issuing Office may further limit participation in the best-and-final offers process to those remaining responsible Offerors that the Issuing Office has, within its discretion, determined to be within the top competitive range of responsive proposals.

C. The Evaluation Criteria described in **Part III, Section III-3**, shall also be used to evaluate the best-and-final offers.

D. Price reductions offered through any best-and-final offer shall have no effect upon the Offeror's Technical Submittal.

I-20. News Releases

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

I-21. Restriction of Contact

From the issue date of this RFP until the Issuing Office selects a proposal for award, the Issuing Officer is the sole point of contact concerning this RFP. Any violation of this condition may cause the Issuing Office to reject the offending Offeror's proposal. If the Issuing Office later discovers that the Offeror has engaged in any violations of this condition, the Issuing Office may reject the offending Offeror's proposal or rescind its contract award pursuant to terms and conditions. Offerors must agree not to distribute any part of their proposals beyond the Issuing Office. An Offeror who shares information contained in its proposal with other Treasury personnel and/or competing Offeror personnel may be disqualified.

I-22. Term of Contract

The contract is a four-year contract, beginning upon execution with a target date of February 28, 2026, with four optional one–year renewal periods. Treasury can choose to renew the contract for each optional renewal period, or it can choose to renew all optional renewal periods at once. The Contract must grant to Treasury sole discretion to determine the exercise of renewal options, if any, in single or multiple year increments. The Effective Date for the Contract shall be the date of the last signature required to create a legally binding Contract with the Commonwealth (which will be the signature of a designated official of the Pennsylvania Office of Attorney General). The Offeror shall not start the performance of any work prior to authorization by Treasury.

I-23. Responsible and Responsive Defined

For definitions, please see Section I-19.B.i.

I-24. Offeror's Representations and Authorizations

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

A. All the Offeror's information and representations in the proposal are material and important, and the Issuing Office may rely upon the contents of the proposal in awarding the Contract(s). The Commonwealth shall treat any mistake, omission or misrepresentation as fraudulent concealment of the true facts relating to the Proposal submission, punishable pursuant to 18 Pa. C.S. § 4904.

B. The Offeror has arrived at the price(s) and amounts in its proposal independently and without consultation, communication, or agreement with any other Offeror or potential Offeror.

C. The Offeror has not disclosed the price(s), the amount of the proposal, or the approximate price(s) or amount(s) of its proposal to any other firm or person who is an Offeror or potential Offeror for this RFP. The Offeror shall not disclose any of these items until a vendor is selected for negotiations.

D. The Offeror has not attempted, nor will it attempt, to induce any firm or person to refrain from submitting a proposal on this Contract, or to submit a proposal higher than its proposal, or to submit any intentionally high or noncompetitive proposal or other form of complementary proposal.

E. The Offeror makes its proposal in good faith and not pursuant to any agreement or discussion with, or inducement from, any firm or person to submit a coordinated, complementary, or otherwise noncompetitive proposal.

F. To the best knowledge of the person signing the proposal for the Offeror, the Offeror, its affiliates, subsidiaries, officers, directors, and employees are not currently under investigation by any government agency and have not in the last four (4) years been convicted or found liable for any act prohibited by State or Federal law in any jurisdiction involving conspiracy or collusion with respect to bidding or proposing on any public Contract, except as the Offeror has disclosed in its proposal.

G. To the best of the knowledge of the person signing the proposal for the Offeror, and except as the Offeror has otherwise disclosed in its proposal, the Offeror has no outstanding delinquent obligations to the Commonwealth including, but not limited to, any state tax liability not being contested on appeal or other obligation of the Offeror that is owed to the Commonwealth.

H. The Offeror is certifying that it is not currently under suspension or debarment by the Commonwealth, any other State, or the Federal government, and if the Offeror cannot certify, then it shall submit along with its proposal a written explanation of why it cannot make such certification.

I. The Offeror has not made, under separate Contract with the Issuing Office or otherwise, any recommendations to the Issuing Office concerning the need for the services described in its proposal or the specifications for the services described in the proposal.

J. The Offeror, by submitting its proposal, authorizes Commonwealth agencies to release to Treasury information concerning the Offeror's Pennsylvania taxes, Unemployment Compensation and Workers' Compensation liabilities.

K. Until the Offeror receives a fully executed and approved written Contract from the Issuing Office, there is no legal and valid Contract, in law or in equity.

I-25. Notification of RFP Outcome

A. **Contract Negotiations**. Pursuant to **Part I, Section I-5**, the successful bidder will be notified when they are selected for contract negotiations.

B. **Award**. Offerors whose proposals are not selected will be notified when Contract negotiations have been successfully completed, and the Issuing Office has awarded the final negotiated and fully executed Contract to the selected Offeror.

I-26. Debriefing Conferences

Upon notification of the award, Offerors whose proposals were not selected will be given the opportunity to be debriefed. The Issuing Office will schedule each debriefing at a mutually agreeable time. The debriefing will not compare the Offeror with other specifically named Offerors, other than the position of the Offeror's proposal in relation to all other Offeror proposals. An Offeror's exercise of the opportunity to be debriefed does not constitute, or toll the time for, filing a protest (See Section I-27 of this RFP).

I-27. RFP Protest Procedure

Protest Procedures for this RFP are attached - **Appendix F**.

I-28. Use of Electronic Versions of this RFP

This RFP is being made available by electronic means. If an Offeror electronically accepts the RFP, the Offeror acknowledges and accepts full responsibility to monitor the RFP to identify any changes made to it (e.g., by way of addenda from the Issuing Office). In the event of a conflict between a version of the RFP in the Offeror's possession and the Issuing Office's version of the RFP, the Issuing Office's version shall govern.

PART II: PROPOSAL REQUIREMENTS

Offerors must submit their proposals in the format, including heading descriptions, outlined below. To be considered, the proposal must respond to all requirements in this part of the RFP. Offerors should provide any other information thought to be relevant, but not applicable to the enumerated categories, as an appendix to the Proposal. All cost data, including Small Diverse Business cost data, should be kept separate from and not included in the Technical Submittal. **If cost information is contained in a technical submittal, such Offeror may be disqualified from this RFP.**

Each Proposal shall consist of the following three (3) separate submittals, sent via 3 separate emails as described in **Part I, I-12**.

A. Technical Submittal, in response to **Part II, Sections II-1 through II-7**.

B. Small Diverse Business participation submittal, in response to **Part II, Section II-8.**

C. Cost Submittal, in response to **Part II, Section II-9**.

The Issuing Office reserves the right to request additional information that, in the Issuing Office's opinion, is necessary to assure that the Offeror's competence, number of qualified employees, business organization, and financial resources are adequate to perform according to the RFP requirements.

The Issuing Office may make inquiries as it deems necessary to determine the ability of the Offeror to perform the requested services. The Offeror shall furnish the Issuing Office with all pertinent information and data, including site visits and requests for additional information. The Issuing Office reserves the right to reject any proposal if the information submitted by such Offeror fails to satisfy the Issuing Office that such Offeror is properly qualified to carry out the obligations of the RFP and to complete the Project as specified.

Technical Submittal (Part II, Sections II-1 to II-7)

An Offeror's response to the information requested in **Part II, Sections II-1 to II-7** constitutes the Technical Submittal. **The Technical Submittal shall be sent in an email as described in Part I, Section I-12, separate from the Small Diverse Business and Cost Submittals.** The Offeror should not include any assumptions in its Technical Submittal unless explicitly stated by Treasury in this RFP. If the Offeror includes assumptions in its technical submittal, the Issuing Office may reject the proposal. Offerors should direct in writing to the Issuing Office pursuant to **Part I, Section I-9**, of this RFP any questions.

II-1. Statement of the Problem

State in concise terms your understanding of the problem presented, or the service required by this RFP by briefly addressing the task descriptions and numbering convention found in **Part II, section II-7** of this RFP (Work Plan) to provide a narrative summary of the Offeror's technical plan for accomplishing the work. Describe how the Offeror's plan will address project management, acceptance testing, quality management, and risk management generally. Treasury is interested in proposals that Offerors will be able to immediately implement upon contract signing. Describe the Offeror's capabilities in promptly implementing a plan.

II-2. Prior Experience

Describe the Offeror's experience in providing reliable colocation data center facility and related services (Current and past). Summarize and provide examples of the scope and services in the performance of these projects. Describe experience in working with large-scale companies or government agencies of similar size and scale. Please provide references.

II-3. Personnel

Provide the qualifications of your management team and staff to host and secure PA Treasury equipment and perform the mandatory requirements specified in the RFP.

II-4. Equipment

Describe the equipment capabilities and capacity to meet the requirements specified in the RFP.

II-5. Financial Capacity, Disclosure of Ongoing Litigation, Corrective Action, and Liquidated Damages

Describe your company's financial stability and economic capability to perform the Contract requirements. Provide your company's financial statements for the past three (3) fiscal years (electronic versions encouraged): If your company is a publicly traded company, please provide a link to your financial records on your company website; otherwise, provide three (3) years of your company's financial documents such as audited financial statements or recent tax returns. Financial statements must include the company's Balance Sheet and Income Statement or Profit/Loss Statements.

The Offeror must include the disclosure of any ongoing litigation or any adverse actions (e.g., Contract termination, corrective action, liquidated or actual damages, regulatory action) against it within the past five (5) years from any governmental organizations for which it has been providing similar services. The disclosure must include the date of initiation, the nature of the litigation or adverse action, the parties involved in the action, and, if resolved, the resolution.

II-6. Objections and Additions to Standard Contract Terms and Conditions

An Offeror should explicitly acknowledge that its proposal is submitted based upon acceptance of the Standard Contract Terms and Conditions ("Standard Terms") set out in **Appendix A** as well as the Information Security Addendum set out in **Appendix C**.

The Offeror may also propose, in full, provisions it wishes to add to the Standard Terms if it is selected for Contract negotiations. The Offeror shall similarly provide a rationale for proposed additional terms. The Issuing Office will not accept references to the Offeror's, or any other, online guides or online terms and conditions contained in any other proposal or Contract.

The Issuing Office may, in its sole discretion, accept or reject during Contract negotiations any proposed changes to the Standard Terms, including any proposed changes submitted later than the deadline for submission of proposals, if, in the Issuing Office's sole discretion, they would be in the best interest of the Commonwealth. If the Issuing Office rejects a proposed change, the Offeror shall be obligated to accept the respective Standard Term.

II-7. Work Plan

As part of the proposal, Offerors shall submit a work plan that includes a response to each numbered requirement, utilizing the same numbering scheme to facilitate evaluation. Each Offeror shall confirm its compliance with the Treasury requirements in its response and detail how the Offeror will perform the tasks as described in each section.

Treasury has established certain requirements with respect to its evaluation of proposals submitted by Offerors. The use of "shall," "must," or "will" in the RFP indicates a requirement or condition that is mandatory. An Offeror failing to meet a mandatory Treasury requirement or providing a response that materially deviates from the mandatory requirement can result in Treasury awarding zero (0) points in the scoring phase for the applicable section of the proposal and may lead to the proposal not receiving many of the available points on a highly weighted component of the proposal. Treasury may waive a mandatory requirement or condition in its sole discretion if an Offeror fails to meet it but provides a reasonable basis for its deviation from the prescribed requirement or condition, and Treasury determines that the deviation is not material. A deviation from a requirement or condition is material if Treasury determines the deficient response does not substantially comply with the RFP requirement or condition, providing an advantage to one Offeror over other Offerors.

The words "should," "may," or "encouraged" in the RFP indicate desirable attributes or conditions but are non-mandatory in nature. Deviation from, or omission of, such a desirable feature will decrease the number of points that a proposal will receive for that feature, but the Offeror will remain eligible to receive partial points for its response.

A. Administration

1. The Offeror shall identify a full-time Contract Manager and a backup manager; it will appoint for its Contract with Treasury. The Contract Manager shall be a designated individual with analytical skills, judgment, experience, and authority to respond to inquiries from designated Commonwealth staff on tasks including but not limited to Contract compliance and delivery of services.

2. The Offeror must procure and maintain, at its expense, and require its Subcontractors to procure and maintain, as appropriate, the following types of insurance, issued by companies acceptable to the Commonwealth and authorized to conduct such business under the laws of the Commonwealth of Pennsylvania:

a. Workers' Compensation insurance in accordance with the Workers' Compensation Act (77 P.S. §1 et seq.). The Offeror shall ensure that its Subcontractors also comply with this requirement.

b Commercial General Liability insurance to protect the Commonwealth, as additional insured, and the Offeror from claims for damages including, but not limited to personal injury (including bodily injury), accidental death, and damages (including property damage), which may arise from its operations under this Contract. The Offeror should have limits of no less than five million dollars ($5,000,000). Such policies shall be occurrence rather than claims-made policies and shall name the Commonwealth of Pennsylvania as an additional insured.

c) Errors and Omissions insurance with limits of not less than five million dollars ($5,000,000) per claims-made basis shall be maintained throughout the duration of the Contract. The Offeror shall ensure that its Subcontractors comply with this requirement.

d) Fidelity/Commercial Crime insurance covering the loss that may be incurred due to loss of money, securities, or inventory resulting from crime, including burglary, robbery, theft, disappearance destruction or embezzlement by the Offeror or employees of Offeror. Fidelity/Commercial Crime insurance with limits of not less than five million dollars ($5,000,000) per loss shall be in full force throughout the term of the Contract and shall name the Commonwealth of Pennsylvania as a joint loss payee as its interests may appear. The Offeror shall ensure that its Subcontractors comply with this requirement.

e) Offeror will provide the Commonwealth of Pennsylvania with a standard ACORD form certificate as evidence of insurance coverage within ten (10) days of Contract award. Offeror will provide updated certificates annually. Additionally, the Offeror will provide updated ACORD forms evidencing continuing coverage of the insurance requirements upon expiration of the previous ACORD forms.

3. The Offeror shall hold the Commonwealth harmless and indemnify the Commonwealth against any and all claims, demands or actions based upon or arising out of any activities performed by the Offeror or its employees or agents, including Subcontractors, under any Contract resulting from this RFP and shall, at the request of the Commonwealth, defend any and all actions brought against the Commonwealth based on any such claims or demands. The Commonwealth will not indemnify the Offeror.

4. Treasury reserves the right to inspect the facilities of the Offeror, including those of Subcontractors, to ensure compliance with all required services outlined in this RFP. The Issuing Office reserves the right to restrict onsite visits to the remaining responsible Offerors that it has determined, at its discretion, to be within the top competitive range of responsive proposals.

B. Confidentiality, Security, and Data Management

1. All security measures as specified in the Contract must be always maintained. Treasury considers any breach of confidentiality/security, including instances in which confidential information is exposed to unauthorized access or examination even without evidence that any information was copied or otherwise "taken," a material breach of any Contract resulting from this RFP. Any breach may result in Treasury's termination of the Contract.

2. The Offeror must describe their processes and procedures, and those of their subcontractors, that will be used to ensure the confidentiality of information and how information is protected, including, but not limited to, the following measures:

a) Describe how information will be restricted to those individuals whose access is essential to the administration of services.

b) Describe how individuals with physical access to Treasury equipment will be under the supervision and control of the Offeror.

c) Describe how the Offeror will ensure that any Subcontractors will be bound by the same confidentiality requirements as the Offeror.

3. Describe the procedures used by Offeror to resolve (prosecute) fraud and/or criminal activity, how and when the Offeror will notify Treasury, and what information will be provided.

4. The Offeror must describe the procedures for lost, stolen, or damaged equipment.

5. The Offeror must provide a limited number of designated Treasury staff internet connectivity during on-site visits, and system compatibility/ access.

6. The Offeror shall explain whether the Offeror would use its own employees or sub-contract the responsibility to a third party. Note: SOC report may be required for third-party contracts.

7. The Offeror will provide other information it deems relevant and necessary to a comprehensive proposal.

C. Reporting and Auditing

1. The Offeror shall describe how it will provide Treasury with detailed reporting and query functions to the maximum extent permissible under Federal and State regulations in an electronic format approved by Treasury. The Offeror must submit in its proposal samples of required reports (as specified below) as well as of any additional reports it will make available.

2. The Offeror shall ensure that any reports requested by Treasury are available in summary and detailed formats. Reports must be delivered to Treasury electronically in a format approved by Treasury. Treasury requests the latest SOC 2 report (or an equivalent attestation) as well as the latest audited financial statement.

D. Disaster Recovery/Business Continuation

1. The Offeror must include a plan for business continuation and/or recovery as a response to the threat of disaster. The disaster recovery plan is complementary to the Offeror's normal security and emergency preparedness plans. A disaster is defined as a full or partial loss of the facility due to a catastrophic event which causes vital business processes to stop. A disaster may be caused by:

a) An event resulting in the inability to meet important customer commitments and contractual obligations or to protect the interests of Treasury and the Offeror and its employees.

b) The catastrophic loss of system/service and/or degradation due to, but not limited to:

i. Power outage.
ii. Server failure.
iii. Router failure.
iv. Cable failure.
v. Power surge.
vi. Internet failure.
vii. Virtual private network (VPN) failure.
viii. Computer virus/ malware/ ransomware.
ix. Inability to access data or operations stored or performed remotely (e.g., cloud storage or computing) or failure of remote functionality to perform as required.
x. Any other similar factor or event that results in catastrophic loss.
xi. Fire, flood, natural disaster, etc.

2. Describe the Offeror's disaster recovery and continuation of business plan. Include backup procedures for your management systems (Access control & surveillance monitoring), alternate operating facilities, hardware and software replacement, and testing procedures and history. Please include a description of the readiness status of alternate facilities (e.g., explain whether they are hot sites, cold sites, other) as well as identification of the location of those facilities and whether they are owned by the Offeror or secured via Contract. The description should include expected recovery times and explain, if applicable, how the Offeror determines which facilities to utilize based upon the nature and severity of a disaster. If the Offeror must relocate operations because of disaster, describe in detail how Treasury assets and infrastructure would be prioritized.

3. Outline the rapid notification procedures when operational failures occur.

4. Describe how procedure manuals are made available during a disaster (electronic and/or print).

5. All Treasury contacts, members of each of the disaster recovery plan teams, and other appropriate Offeror staff must be kept up to date during an offeror disaster. The Offeror must describe in its proposal how it will continue to communicate with Treasury during a disaster and provide information about (1) when services will be reestablished, (2) any decision to re-locate to an alternate facility, and (3) all other matters. Treasury strongly believes that communication with staff, customers, and Treasury contacts is crucial to the actual and perceived success of the recovery efforts.

E. End of Contract Activities

Upon expiration of the Contract, or termination for any reason before the end of the Contract term, the Offeror must, upon request by Treasury, extend the services to facilitate transition to a new services provider for a period to be by and at the sole discretion of Treasury, but not for a **period to exceed 180 days**.

Small Diverse Business Participation Submittal (Part II, Section II-8)

The information requested in **Part II, Section II-8**, shall constitute the Small Diverse Business Participation Submittal. The Small Diverse Business Participation Submittal shall be sent via email to RFP25-002@patreasury.gov as described in **Part I, Section 1-12**, separate from the Technical and Cost Submittals. Offerors should direct any questions in writing to the Issuing Office pursuant to **Part I, Section I-9**, of this RFP.

A maximum of five (5) points may be awarded for this section.

II-8. Small Diverse Business and Veteran Business Enterprise Submittal

The Offeror's Small Diverse Business (SDB) and Veteran Business Enterprise (VBE) Participation Submittal shall include acknowledgment and a response to each item below.

A. If the Offeror has self-certified as a Small Diverse Business in accordance with the requirements established by the Department of General Services (DGS) Pennsylvania Bureau of

Diversity, Inclusion and Small Business Opportunities ("BDISBO"), has also been verified as a Small Diverse Business by one of the DGS' third-party certifiers, and been included on the DGS on-line database (http://www.dgs.internet.state.pa.us/suppliersearch), it must submit evidence of its Small Diverse Business qualification. The Offeror shall provide proof of qualification in the form of the certification provided by the third-party certifier and a screen shot showing its inclusion on the DGS database.

Likewise, if the Offeror is claiming VBE eligibility, then verification through the above website is required.

B. To support its Small Diverse Business Subcontractor commitment, the Offeror must also include:

1. The name, mailing address, email address, and telephone number of the primary contact person of each Small Diverse Business to which a commitment is made by the Offeror. The Offeror will not receive credit for stating that it will find a Small Diverse Business after Contract award.

2. Proof of Small Diverse Business's qualification for each Small Diverse Business to which a commitment is being made by the Offeror. Proof of a Subcontractor's qualification shall be provided in the same manner as required for proof from the Offeror, as described in **Part II, Section II-8. A.**

If an Offeror, submitting letters of intent regarding one or more Small Diverse Businesses, is selected for negotiations, the Offeror will be required to provide conforming signed subcontracts with the Small Diverse Business (or Businesses) prior to final Contract execution.

Cost Submittal (Part II, Section II-9)

The information requested in **Part II, Section II-9**, shall constitute the Cost Submittal. The Cost Submittal shall be sent via email to RFP25-002@patreasury.gov as described in **Part I, Section 1-12**, separate from the Technical and Small Diverse Business Participation Submittals.

Except for it being necessary to respond to the request for information about other programs, no component of an Offeror's Cost Submittal shall be made conditional, or otherwise provisional, based upon the accuracy of validity of any assumption the Offeror makes in preparing its proposal. Treasury does not encourage an Offeror to explicitly disclose any assumption it relied upon in preparing its Cost Submittal. Any attempt by an Offeror to make a component of its proposal conditional or provisional may result in the Issuing Office rejecting the Offeror's proposal.

II-9. Cost Submittal

Please refer to the Cost Proposal Sheet in **Appendix E**.

Cost proposals shall be submitted using the Cost Proposal Submission Sheet in **Appendix E** of this RFP. You may include additional explanations for costs on subsequent sheets. Those explanations must be included only with the Vendor's cost proposal inclusion with the Technical Proposal Submission.

PART III: CRITERIA FOR SELECTION

A Department selected Advisory Committee will review and evaluate all written proposals submitted by the deadline based on the criteria identified in this solicitation. Late submittals will be rejected without opening.

III-1. Mandatory Requirements

To be considered responsive, a proposal must be:

A. Timely received from the Offeror according to the RFP **Calendar of Events**.

B. Correctly submitted using the format in **Part I, section I-12** (absolutely no costs may be discussed in the Technical and Small Diverse Business submittals).

C. Submitted with signed **Proposal Cover Sheet Appendix D**.

III-2. Evaluation

The Issuing Office has selected a committee of qualified personnel to review and evaluate timely submitted proposals ("Proposal Evaluation Team"). The Issuing Office will notify in writing of its selection for negotiation of the responsible Offeror (as defined by **Section I.19.B**.) whose proposal is determined to be the most advantageous to the Commonwealth as determined by the Issuing Office after taking into consideration all the evaluation factors. While the Issuing Office generally selects a single Offeror with which to begin negotiations, it reserves the right to enter negotiations with multiple Offerors.

III-3. Evaluation Criteria

Only those proposals that receive enough of the evaluation points allocated to the Technical Submittal i.e., **Part II, Sections II-1 to II-7**, will be eligible for further consideration. Proposals that include the Offeror's acknowledgement and acceptance of each Treasury requirement specified to be included in the Technical Submittal of this RFP are more likely to receive a competitive score.

Tier compliance is a critical requirement of this RFP. Vendors without the capability to meet a minimum of Tier 3 compliance according to Treasury standards will not be evaluated.

III-4. Offeror Responsibilities

An Offeror must submit a responsive proposal (as defined in **Section I.19.B**.) and possess the capability to fully perform the Contract requirements in all respects and the integrity and reliability to assure good faith performance of the Contract.

For an Offeror to be considered responsible for this RFP, and therefore eligible for selection for a site visit, best-and-final offers, or selection for Contract negotiations:

A. The total score for the technical submittal of the Offeror's proposal must be within the top competitive range of responsive proposals.

B. The Offeror's financial information must demonstrate that the Offeror possesses the financial capability to assure good-faith performance of the Contract. The Issuing Office will review the Offeror's previous three (3) financial statements, any additional information received from the Offeror, and any other publicly available financial information concerning the Offeror and assess each Offeror's financial capacity based on calculating and analyzing various financial ratios, and by comparison with industry standards and trends. This is a pass/fail requirement; Offerors will not be compared against each other for this requirement or scored proportionally.

Further, the Issuing Office will award a Contract only to an Offeror determined to be responsible in accordance with the most current version of the Commonwealth's Contractor Responsibility Program, which can be found at
https://www.budget.pa.gov/Programs/Pages/ContractorResponsibilityProgram.aspx
Before Cost Proposals are opened, the Proposal Evaluation Team will review the Technical Response Evaluation record and any other available information pertinent to whether each Offeror is responsive and responsible. If the Proposal Evaluation Team identifies any Offeror that does not meet the responsive and responsible thresholds such that the team would not recommend the Offeror for Cost Proposal Evaluation and potential contract award, the team members will fully document the determination.

PART IV: WORK STATEMENT

IV-1. Objectives

Treasury is soliciting proposals from Offerors having experience and abilities in the areas identified in the Request for Proposal (RFP). Each Proposal must contain evidence of the Offeror's qualifications in the specified areas and in other disciplines directly related to the proposed work.

IV-2. Nature and Scope of the Project

The Pennsylvania Treasury is committed to ensuring uninterrupted mission-critical operations, safeguarding resiliency, and maintaining continuity in the face of unforeseen disruptions. This RFP invites proposals from experienced and financially sound vendors for the design, construction, and operation of a Disaster Recovery Data Center. The new facility must serve as a fully redundant backup location that is geographically diversified relative to our primary data center in Harrisburg, PA.

Key Objectives

- **Resiliency:** To establish a facility capable of seamless failover during emergencies.
- **Regulatory Compliance:** To ensure adherence to all applicable industry and governmental standards.
- **Security & Continuity:** To provide robust physical, cyber, and personnel security measures that guarantee data integrity and operational availability.
- **Scalability & Futureproofing:** To design an infrastructure that is fit for current requirements and adaptable to future technological enhancements and evolving threat landscapes.

The selected vendor shall provide a turnkey solution that includes the design, deployment, management, and maintenance of a disaster recovery data center.

The comprehensive scope is divided into the following functional areas:

Facility Infrastructure

1. Data Center Construction & Colocation:

a. Provide colocation space within a state-of-the-art facility that complies with **Uptime Institute Tier III** (or higher) standards.

b. Ensure that the facility supports concurrent maintainability, allowing scheduled maintenance without service interruption.

c. Submit detailed blueprints, layouts, and capacity planning documents.

2. Location Requirements:

a. The facility must be located within a geographic radius of a minimum of 50 miles and a maximum of 150 miles from our primary data center in Harrisburg, PA.

b. Provide a GIS map detailing the site's relative position with respect to critical infrastructure, highways, and local risk factors.

Technical Infrastructure Requirements

1. **Space & Power Provisions:**

a. Clearly detail the types of collocations available (e.g., individual rack space, dedicated cages, or private suites).

b. Specify power availability, noting kW per rack and the overall available facility capacity.

c. Describe redundant power feeds, backup generators, and Uninterruptible Power Supply (UPS) systems – including specified switching times and failover procedures.

2. **Network Connectivity:**

a. Provide detailed architecture incorporating diverse and redundant network paths.

b. Specify connectivity details such as the use of multiple carriers, fiber route diversity, and scalability of bandwidth.

c. Include performance metrics—latency, jitter, packet loss thresholds, and guaranteed Service Level Agreements (SLAs).

d. Supply network diagrams illustrating redundancy, failover configurations, and traffic management.

Security & Access Controls

1. **Physical Security:**

a. Provide 24x7x365 on-site security with real-time monitoring.

b. Implement multi-factor access controls, including mantrap entry systems, biometric verification, and mandatory photo-ID checks.

c. Ensure comprehensive CCTV coverage with continuous recording and remote monitoring capabilities.

2. **Cyber & Logical Security:**
    a. Enforce secure network segmentation, employ enterprise-grade firewalls, and integrate intrusion detection/prevention systems (IDS/IPS).
    b. Detail data encryption protocols for both data at rest and in transit.
    c. Comply with the attached IT Security Addendum (see Section 3.9).
    d. Include detailed documentation of secure VPN connectivity and remote management protocols.

3. **Visitor & Contractor Management:**
    a. Maintain rigorous logging, screening, and escort policies for third-party personnel.
    b. Ensure audit trails and timestamped entry/exit logs are maintained and available for review.

Environmental & Safety Controls

1. **Environmental Monitoring:**
    a. Deploy HVAC systems capable of precise environmental control for temperature and humidity.
    b. Integrate environmental sensors to continuously monitor air quality, particulate matter, water leaks, and other potential hazards.

2. **Fire Suppression & Safety:**
    a. Install fire detection and suppression systems in compliance with NFPA standards (preferably clean agent or pre-action sprinkler systems).
    b. Provide emergency exit strategies, detailed smoke/heat detection zones, and fail-safe alarm systems.
    c. Include documentation confirming regular maintenance and testing of fire suppression systems.

Office & Disaster Recovery Operations Support

1. **Disaster Recovery Workspace:**
    a. Provide dedicated office space to accommodate up to 20 personnel during a disaster event.
    b. Equip the workspace with individual workstations, network connectivity (wired and wireless), docking stations, and secure data storage.
    c. Include designated conference facilities with video conferencing capabilities, as well as essential office amenities (e.g., printers, telephones).

2. **Operational Readiness & Support Services:**
    a. Offer remote hands-on support and on-demand engineering expertise.
    b. Outline managed service options for data center monitoring, incident response, and routine maintenance.
    c. Supply documented Standard Operating Procedures (SOPs) and emergency playbooks for crisis management.

IV-3. Contract Requirements

The Offeror must be able to provide a reliable colocation data center facility and related services. These services are essential to Treasury's ability to operate seamlessly if/when disaster strikes the primary data center located in Harrisburg, Pennsylvania.

The Offeror must demonstrate or describe in its proposal how it will meet the detailed requirements and specifications which are divided into the following functional areas:

Data Center Tier Classification

1. **Standard of Compliance:**
   a. The facility must meet the Uptime Institute's Tier III classification or equivalent standards, ensuring concurrent maintainability (See Appendix G – Data Center Tier Summary).

2. **Certification:**
   a. Provide an official Uptime Institute Tier III Certification of Compliance.
   b. In lieu of certification, you must provide the most recent detailed performance tests, independent audit reports, and equivalent validation documentation

Location & Geographical Diversification

1. **Distance & Risk Mitigation:**
   a. The facility must be located between 50 and 150 miles from Harrisburg, PA to provide geographical diversification.
   b. Attach a risk assessment report detailing local natural hazards (e.g., flood zones, seismic activity) and your strategies to mitigate these risks.
   c. Provide maps, site surveys, and any relevant environmental reports.

Space and Power Detailed Specifications

1. **Colocation Space:**
   a. Must have adequate space for two racks (42U minimum) – Expandable to four.
   b. Must have minimum of two Power Distribution Unit's (PDU) per rack from different power sources.
   c. Must have front & back rack doors with integrated security.
   d. Provide precise descriptions of the available physical space, identified in square footage, rack units, and any weight load limitations.
   e. Attach schematics that designate areas for IT equipment, support systems, and ancillary functions.

2. **Electrical Infrastructure:**
   a. Detail the total available power in kW, including power density metrics per rack.

b. Describe the redundancy of electrical feed along with emergency power source specifications (Generators, UPS, Etc.).
c. Supply diagrams mapping power distribution layouts and UPS configurations.

Network Architecture & Connectivity Requirements

1. **Connectivity Infrastructure:**
   a. Provide a detailed description of the redundant network architecture, including the model for multi-carrier and multi-path routing.
   b. Include comprehensive network diagrams showing firewalls, routers, load balancing, and routing convergence mechanisms.

2. **Performance Metrics:**
   a. Define SLA thresholds for latency, bandwidth throughput, and jitter.
   b. Supply historical performance data and details on provisions for bandwidth scaling during crises.
   c. Explain maintenance windows and procedures that ensure minimal interruption during upgrades or routine maintenance.

Security Architecture & Protocols

1. **Physical Security Components:**
   a. Specify the number of on-site security personnel and detail the surveillance systems (CCTV placement, recording duration, monitoring protocols).
   b. Provide schematics of access-controlled entry points showing mantrap designs and biometric/ID verification stations.

2. **Cybersecurity Measures:**
   a. Elaborate on technical safeguards, including network segmentation, firewall technologies, encryption protocols, and endpoint protection mechanisms.
   b. Supply incident response flowcharts and past case studies outlining quick notification, containment, and remediation efforts.

Environmental Controls & Fire Safety

1. **Climate Management Systems:**
   a. Provide detailed HVAC system specifications, including energy efficiency ratios (e.g., Power Usage Effectiveness (PUE)), redundancy measures, and preventive maintenance schedules.
   b. Describe the environmental sensor systems used for continuous monitoring of temperature, humidity, and hazardous conditions, including failover alert mechanisms.

2. **Fire Suppression Details:**
   a. Supply technical details and compliance certificates for the installed fire suppression systems.
   b. Provide testing logs and maintenance records for fire safety equipment.
   c. Include diagrams and layouts that indicate the coverage of fire detection and suppression systems within the facility.

Office Workspace and Continuity Operations

1. **Workspace Design:**
   a. Submit detailed floor plans that indicate the layout of the disaster recovery office.
   b. Describe the IT support infrastructure provided within the workspace including network connectivity, data ports, and ergonomic design features.
   c. Describe customer prioritization protocol during regional or multi-customer crisis.

2. **Additional Facilities:**
   a. Include details on ancillary support facilities such as restrooms, break areas, and conference rooms.
   b. Provide specifications for all office equipment and furnishings intended for prolonged operational use in a disaster scenario.

Regulatory Compliance & Certification

1. **Certifications & Attestations:**
   a. Provide proof of any current certifications for the following (or their international/regional equivalents):
      - ISO 27001 – Information Security Management.
      - HIPAA/HITECH – Health Information Protection.
      - PCI DSS v3.2.1 – Payment Card Industry Data Security.
      - NIST SP 800-53 – Security and Privacy for Information Systems.
      - SOC 2 + HITRUST – Combined controls for cybersecurity.

      Note: Any additional regional or government-mandated standards.
   b. Include detailed third-party audit summaries and compliance attestations.
      - SOC 1 Type II & SOC 2 Type II – Service Organization Controls

IT Security Addendum

1. **Mandatory Terms:**
   a. Must sign and strictly adhere to the IT Security Addendum (Exhibit A).
   b. Detail any proposed modifications along with a justification showing that overall security measures remain uncompromised.
   c. Acknowledge that any deviation must be pre-approved by PA Treasury.

Financial Stability & Vendor Qualifications

1. **Financial Documentation:**
   a. Provide audited financial statements covering the past three fiscal years.
   b. Include supporting documents verifying the absence of bankruptcies, liens, or insolvency events in the last ten years.
   c. Supply any relevant credit ratings and financial stability reports from recognized financial institutions.

2. **Experience & Past Performance:**
   a. Submit a detailed company profile describing your history in providing disaster recovery or high-availability data center solutions.

b. Include descriptions of similar projects, with references to current/past clients, contract values, and detailed outcomes.
c. Provide at least three customer references of comparable size (200+ employees with budget exceeding $20 million) and scope along with contact information and written testimonials. At least one reference must be from a government entity (Local, state or federal).

Exclusions

1. **Equipment Ownership:**
   a. All server and IT equipment necessary for mission-critical operations during a disaster recovery event shall be provided by PA Treasury.
   b. Proposals must exclude any server rental or purchase costs.

2. **Non-Core Services:**
   a. Do not include extraneous services outside the defined scope (e.g., end-user device management unless explicitly requested).

SERVICE PURCHASE CONTRACT
TERMS AND CONDITIONS

The following Terms and Conditions apply to a Pennsylvania Treasury Department ("Treasury"), Service Purchase Contract ("Contract") and shall apply in full to Contractor.

1. TERM OF CONTRACT

The term of the Contract shall commence on the Effective Date (as defined below) and shall end on the Expiration Date identified in the Contract, subject to the Contract's specific provisions.

The Effective Date shall be: a) the Effective Date printed on the Contract after the Contract has been fully executed by the Contractor and Treasury (signed and approved as required by Commonwealth contracting procedures) or b) the "Valid from" date printed on the Contract, whichever is later.

2. AUTHORITY

The Contractor shall only have the express authority granted to it this Contract.

3. EXTENSION OF CONTRACT TERM

Treasury reserves the right, upon notice to the Contractor, to extend the term of the Contract upon the same terms and conditions.

4. SIGNATURES

The Contract shall not be a legally binding until fully-executed and has been sent to the Contractor. No Treasury employee has the authority to verbally direct the commencement of any work or delivery of any supply under this Contract prior to the Effective Date. Contractor hereby waives any claim or cause of action for any service or work performed prior to the Effective Date.

The Contract may be electronically signed by Treasury. The electronically-printed name of the applicable Treasury employee represents the signature of that individual who has the authority, on behalf of the Commonwealth, to bind Treasury to the terms of the Contract. A fully-executed Treasury contract may require multiple signatures including that of the Treasury's Office of Chief Counsel and the Pennsylvania Office of Attorney General. Treasury should inform and a Contractor may ask what signature are required by Treasury to execute a specific Contract.

The fully-executed Contract may be sent to the Contractor electronically. The electronic transmission of the Contract shall require acknowledgement of receipt of the transmission by the Contractor. Receipt of the electronic fully executed Contract by the Contractor shall constitute receipt of the fully-executed Contract.

Treasury and the Contractor specifically agree as follows:

a. No handwritten signature shall be required in order for the Contract to be legally enforceable.

b. The parties agree that no writing shall be required in order to make the Contract legally binding, notwithstanding contrary requirements in any law. The parties hereby agree not to contest the validity or enforceability of a genuine Contract or acknowledgement issued electronically under the provisions of a statute of frauds or any other applicable law relating to whether certain agreements be in writing and signed by the party bound thereby. Any genuine Contract or

acknowledgement issued electronically, if introduced as evidence on paper in any judicial, arbitration, mediation, or administrative proceedings, will be admissible as between the parties to the same extent and under the same conditions as other business records originated and maintained in documentary form. Neither party shall contest the admissibility of copies of a genuine Contract or acknowledgements under either the business records exception to the hearsay rule or the best evidence rule on the basis that the Contract or acknowledgement were not in writing or signed by the parties. A Contract or acknowledgment shall be deemed to be genuine for all purposes if it is transmitted to the location designated for such documents.

c. Each party will immediately take steps to verify any document that appears to be obviously garbled in transmission or improperly formatted to include re-transmission of any such document if necessary.

5. INDEPENDENT CONTRACTOR

In performing its obligations under the Contract, the Contractor will act as an independent contractor and not as an employee of Treasury. The Contractor will be responsible for all services in this Contract whether or not Contractor provides them directly. Further, the Contractor is the sole point of contact with regard to all contractual matters, including payment of any and all charges resulting from the Contract.

6. DELIVERY

a. **Supplies Delivery:** All item(s) shall be delivered F.O.B. Destination. The Contractor agrees to bear the risk of loss, injury, or destruction of the item(s) ordered prior to receipt of the items by Treasury. Such loss, injury, or destruction shall not release the Contractor from any contractual obligations. Except as otherwise provided in this contract, all item(s) must be delivered within the time period specified. Time is of the essence and, in addition to any other remedies, the Contract is subject to termination for failure to deliver as specified. Unless otherwise stated in this Contract, delivery must be made within thirty (30) days after the Effective Date.

b. **Delivery of Services:** The Contractor shall proceed with all due diligence in the performance of the services with qualified personnel, in accordance with the completion criteria set forth in the Contract.

7. ESTIMATED QUANTITIES

It shall be understood and agreed that any quantities listed in the Contract are estimated only and may be increased or decreased in accordance with the actual requirements of Treasury and that Treasury in accepting any bid or portion thereof, contracts only and agrees to purchase only the materials and services in such quantities as represent the actual requirements of Treasury. Treasury reserves the right to purchase materials and services covered under the Contract through a separate procurement, whenever Treasury deems it to be in its best interest.

8. WARRANTY

The Contractor warrants that all items furnished and all work or services performed by the Contractor, its agents and subcontractors shall be free and clear of any defects in workmanship or materials. Unless otherwise stated in the Contract, all items are warranted for a period of one year, or for such longer period as may be required in the Contract, following delivery by the Contractor and acceptance by the

Commonwealth. The Contractor shall repair, replace or otherwise correct any problem with the delivered item or the work or services performed hereunder. When an item is replaced, it shall be replaced with an item of equivalent or superior quality without any additional cost to Treasury.

9. OWNERSHIP RIGHTS

a. Treasury retains ownership of all data, records, reports and information delivered or shared with Contractor in order for the Contractor to perform under the Contract.
b. Treasury shall have unrestricted authority to reproduce, distribute, and use any submitted report, data, or material, and any software or modifications and any associated documentation that is designed or developed and delivered to Treasury as part of the performance of the Contract.
c. Treasury shall own all Developed Works or Developed Materials which are defined as: All documents, sketches, drawings, designs, works, papers, files, reports, computer programs, computer documentation, data, records, software, samples or any other tangible material without limitation authored or prepared by Contractor as the work product covered in the scope of work for the Project.

10. COMPENSATION

a. **Compensation for Supplies:** The Contractor shall be required to furnish the awarded item(s) at the price(s) quoted in the Contract. All item(s) shall be delivered within the time period(s) specified in the Contract. The Contractor shall be compensated only for item(s) that are delivered and accepted by Treasury.
b. **Compensation for Services:** The Contractor shall be required to perform the specified services at the price(s) quoted in the Contract. All services shall be performed within the time period(s) specified in the Contract. The Contractor shall be compensated only for work performed to the satisfaction of the Commonwealth. The Contractor shall not be allowed or paid travel or per diem expenses except as specifically set forth in the Contract.

11. INVOICES

All invoices must contain the Contractor's name, address, Tax identification number, description of supplies or services that is sufficient for Treasury to determine what work was performed. To the extent a Contractor is to be paid for work by the hour, Contractor shall provide a detailed hourly description and rate with each invoice. Treasury reserves the right to request invoice clarification and a resubmission.

12. ACH PAYMENT REQUIREMENT

a. Treasury will make payments to Contractors through the Automated Clearing House ("ACH"). Within 10 days of the contract, the Contractor must submit or have already submitted their completed ACH form to the Treasurer's Office of Comptroller at PATreasuryAccountsPayable@patreasury.gov. A blank ACH form will be included with Treasury issued contracts and will also be available for download on Treasury's website under Procurement.
b. Single annual payment Contractors who bill less than $5,000 annually and receive only one payment per year may receive payment by check.
c. Contractors may for good cause opt to receive check payments by sending an e-mail to the Office of Comptroller at PATreasuryAccountsPayable@patreasury.gov and providing an explanation as to why Contractor is unable or unwilling to receive an ACH for payment. Treasury may approve such requests at its sole discretion.
d. Treasury in its sole discretion may elect to pay a Contractor through a means other than ACH.

e. Each Contractor shall submit a unique invoice number with each invoice. The unique invoice number will be listed on the ACH remittance advice to enable the Contractor to properly apply the payment.
f. It is the Contractor's responsibility to ensure that ACH information on file with Treasury is accurate and complete. Contractor's failure to maintain accurate and complete information may cause payment delays.
g. Treasury utilizes fraud protection services, including account verification of information provided by Contractors. If Contractor's ACH information fails an account verification, they will be notified to correct such information and be directed to provide additional identifying information and/or that an alternative payment methodology must be utilized.

13. BUDGET IMPASSE

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

14. WEBSITE USER AGREEMENT PROVISIONS

To the extent that the Contractor utilizes a website user agreement (the "Website User Agreement") in connection with communications with Treasury, the Contractor hereby agrees that such Website User Agreement shall not be binding on the Treasury and the terms, conditions, obligations and duties of the parties shall instead be governed by the Contract Terms and Conditions herein.

15. SOFTWARE LICENSING AGREEMENTS

For any software purchase, the terms and conditions herein apply as does any Commonwealth Licensing Agreement. If there is not an applicable Commonwealth Licensing Agreement, Treasury shall provide Contractor with Treasury's Information Technology Terms and Conditions.

16. BACKGROUND CHECKS

a. The Contractor must, at its expense, arrange for a background check for each of its employees, as well as the employees of any of its subcontractors, who will have access to Treasury or Commonwealth facilities, either through on-site access or through remote access. Background checks are to be conducted via the Request for Criminal Record Check form and procedure found at http://www.psp.state.pa.us/psp/lib/psp/sp4-164.pdf. The background check must be conducted prior to initial access and on an annual basis thereafter.

b. Before Treasury will permit access to the Contractor, the Contractor must provide written confirmation that the background checks have been conducted. If, at any time, it is discovered that a Contractor employee has a criminal record that includes a felony or misdemeanor involving terroristic behavior, violence, use of a lethal weapon, or breach of trust/fiduciary responsibility or which raises concerns about building, system or personal security or is otherwise job-related, the Contractor shall not assign that employee to any Commonwealth facilities, shall remove any access privileges already given to the employee and shall not permit

that employee remote access unless Treasury consents to the access, in writing, prior to the access. Treasury may withhold its consent in its sole discretion. Failure of the Contractor to comply with the terms of this Section on more than one occasion or Contractor's failure to appropriately address any single failure to the satisfaction of Treasury may result in the Contractor being deemed in default of its Contract.

c. Treasury specifically reserves the right to conduct background checks over and above that described herein.

d. Access to certain Capitol Complex buildings and other state office buildings is controlled by means of card readers and secured visitors' entrances. Treasury contracted personnel who have regular and routine business in Commonwealth worksites may be issued a photo identification or access badge subject to the requirements of the contracting agency and DGS set forth in Enclosure 3 of Commonwealth Management Directive 625.10 (Amended) Card Reader and Emergency Response Access to Certain Capitol Complex Buildings and Other State Office Buildings. The requirements, policy and procedures include a processing fee payable by the Contractor for contracted personnel photo identification or access badges.

17. CONFLICT

The Contractor is bound by the terms and conditions of this Contract. The priority of documents for any Contract are as follows:

- The terms and conditions, including appendices, of this Contract including any negotiated attachment
- Any answer or submission by vendor to a procurement issued by the Department;
- A procurement issued by the Department;
- Applicable Statewide Requirements Contract, Invitation To Qualify contract, or Commonwealth Licensing Agreement;
- All other documents.

18. ASSIGNABILITY AND SUBCONTRACTING

a. Subject to the terms and conditions of this Paragraph, this Contract shall be binding upon the parties and their respective successors and assigns.

b. The Contractor shall not subcontract with any person or entity to perform all or any part of the work to be performed under this Contract without the prior written consent of Treasury, which consent may be withheld at the sole and absolute discretion of Treasury.

c. The Contractor may not assign, in whole or in part, this Contract or its rights, duties, obligations, or responsibilities hereunder without the prior written consent of Treasury, which consent may be withheld at the sole and absolute discretion of Treasury.

d. A change of name by the Contractor, following which the Contractor’s federal identification number remains unchanged, shall not be considered to be an assignment hereunder. The Contractor shall give Treasury written notice of any such change of name.

19. CONFIDENTIALITY

The Contractor agrees to guard the confidentiality of all information it comes by through this Contract with the same diligence with which it guards its own proprietary information. If the Contractor needs to disclose all or part of project materials to third parties to assist in the work or service performed for Treasury, it may do so

only if the third-party agrees to the provisions in these Standard Terms and Conditions and any other appendix. Contractors and third-parties may be required to sign an additional Confidentiality Agreement.

20. FORCE MAJEURE

Neither party will incur any liability to the other, or be deemed to have defaulted under or breached the Contract, if its performance of any obligation under this Contract is prevented or delayed by causes beyond its control and without the fault or negligence of either party. Causes beyond a party's control may include, but are not limited to, acts of God or war, subsequent changes in controlling law, regulations, orders or the requirements of any governmental entity, severe weather conditions, civil disorders, natural disasters, fire, epidemics and quarantines, general strikes throughout the trade, and freight embargoes.

The Contractor shall notify the Treasury orally within five (5) days and in writing within ten (10) days of the date on which the Contractor becomes aware, or should have reasonably become aware, that such cause would prevent or delay its performance. Such notification shall (i) describe fully such cause(s) and its effect on performance, (ii) state whether performance under the contract is prevented or delayed and (iii) if performance is delayed, state a reasonable estimate of the duration of the delay. The Contractor shall have the burden of proving that such cause(s) delayed or prevented its performance despite its diligent efforts to perform and shall produce such supporting documentation as Treasury may reasonably request. After receipt of such notification, Treasury may, at Treasury's sole election, terminate the Contract or, alternatively, extend the time for performance as reasonably necessary to compensate for the Contractor's delay.

In the event of a declared emergency by competent governmental authorities, Treasury by notice to the Contractor, may suspend all or a portion of the Contract.

21. TRANSPARENCY COMPLIANCE

Treasury is an agency of the Commonwealth subject to the public records law of the Commonwealth of Pennsylvania, the Right to Know Law ("RTKL"), which provides generally that all records relating to a public agency's business are open to inspection and copying unless specifically exempted. Additionally, contracts over $5,000 must be placed on the Commonwealth's publicly accessible web-library. The Pennsylvania Web Accountability and Transparency Act (the "Penn Watch Act") requires Treasury to also place certain expenses on a publicly available website.

22. JURISDICTION AND CONFLICTS OF LAW

The Contract and all related documents, and all matters arising out of or relating to the Contract, whether sounding in contract, tort, or statute, shall be governed by, and construed in accordance with, the laws of the Commonwealth of Pennsylvania, without giving effect to its conflict of laws principles. The Contractor irrevocably and unconditionally agrees that it will not commence any action, litigation, or proceeding of any kind whatsoever in any way arising from or relating to this Contract and all contemplated transaction, in any forum other than the courts of the Commonwealth of Pennsylvania. The Contractor consents to the exclusive jurisdiction of the courts of the Commonwealth of Pennsylvania, including the Commonwealth Board of Claims, state, and federal courts, and any appellate court from any thereof, waiving any claim or defense that such forum is not convenient or proper. The Contractor agrees that any such courts will have *in personam* jurisdiction over Contractor, and consents to service of process in any manner authorized by Pennsylvania law. The Contractor agrees that a final judgment in any such action, litigation, or proceeding is conclusive and may be enforced in other jurisdictions by suit on the judgment or in any other manner provided by law.

23. INFORMATION TECHNOLOGY

Any contract related to software, information technology related services, or a contracts that involves the access to, usage or storage of Treasury data - including by way of example only, personal identifying information, financial account information, and security information - may include as a required Appendix – Data Security Addendum - to these term and conditions.

24. UNCLAIMED PROPERTY PROVISIONS

Contractor agrees to report and deliver any abandoned or unclaimed property held by Contractor or its agents, subcontractors, or assignees, as defined by and in accordance with the Disposition of Abandoned and Unclaimed Property Act ("DAUPA"), 72 PS § 1301.1 et seq. A negative report must be filed if Contractor determines, after a records review, that there is no reportable unclaimed property.

Instructions and assistance in filing the report are available from the Bureau of Unclaimed Property holder hotline at 1-800-379-3999 or via e-mail at unclaimedpropertyreporting@patreasury.gov. Additional information regarding the Pennsylvania Abandoned and Unclaimed Property Program is located at www.patreasury.gov.

Contractor must cooperate with any unclaimed property examination conducted by Treasury or its outside auditors. Failing to cooperate with such audit may result in cancellation of this Contract.

25. COMMONWEALH HELD HARMLESS

a. The Contractor shall hold Treasury and the Commonwealth harmless from and indemnify the Treasury against any and all third party claims, demands and actions based upon or arising out of any activities performed by the Contractor and its employees, subcontractors, and agents under this Contract.

b. Notwithstanding the above, neither party shall enter into any settlement without the other party's written consent, which shall not be unreasonably withheld. The Commonwealth may, in its sole discretion, allow the Contractor to control the defense and any related settlement negotiations.

26. TERMINATION PROVISIONS

Treasury has the right to terminate this Contract or any Purchase Order for any of the following reasons. Termination shall be effective upon written notice to the Contractor.

a. **TERMINATION FOR CONVENIENCE**: Treasury shall have the right to terminate the Contract for its convenience if Treasury determines termination to be in its best interest. The Contractor shall be paid for work satisfactorily completed prior to the effective date of the termination, but in no event shall the Contractor be entitled to recover loss of profits.

b. **NON-APPROPRIATION**: Treasury's obligation to make payments during any Commonwealth fiscal year succeeding the current fiscal year shall be subject to availability and appropriation of funds. When funds are not appropriated or otherwise made available to support continuation of performance in a subsequent fiscal year period, Treasury shall have the right to terminate the Contract. The Contractor shall be reimbursed for the reasonable value of any nonrecurring costs incurred but not amortized in the price of the supplies or services delivered under the Contract. Such reimbursement shall not include loss of profit, loss of use of money, or administrative or overhead costs. The reimbursement amount may be paid from any appropriations available for that purpose.

c. **TERMINATION FOR CAUSE**: Treasury shall have the right to terminate the Contract for Contractor default upon written notice to the Contractor. Treasury shall also have the right, upon written notice to the Contractor, to terminate the Contract or a Purchase Order for other cause as specified in the Contract or by law. If it is later determined that Treasury erred in terminating the Contract for cause, then, at the Commonwealth's discretion, the Contract shall be deemed to have been terminated for convenience under Subparagraph a.

27. RESERVATION OF IMMUNITIES

Treasury reserves all immunities, defenses, rights, and actions arising from its sovereign status and/or under the Eleventh Amendment to the United States Constitution. Nothing contained in this Agreement shall constitute a waiver of such immunities, defenses, rights or actions. Nothing contained in these Terms shall be construed or interpreted as the consent of Treasury and the Commonwealth of Pennsylvania, their agents and agencies, to be sued except as provided for herein.

28. ASSIGNMENT

Contractor shall not assign any of its rights or delegate any of its obligations under the Contract without prior written consent of Treasury. Any purported assignment or designation in violation of this section is null and void.

29. COMPLIANCE WITH LAW

Contractor is in compliance with and shall comply with all applicable laws, regulations and ordinances. Contractor has and shall maintain in effect all the licenses, permissions, authorizations, consents, and permits required to carry out its obligations under the Contract.

30. SEVERABILITY

If any term or provision of this Contract is held by a court to be invalid, illegal or unenforceable, such invalidity, illegality or unenforceability shall not affect any other term or provision of this Contract, and the Contract shall be construed as if such provision or provisions had never been contained herein.

31. ENTIRE AGREEMENT.

The Contract, including these terms and conditions, and the agreements referred to in or contemplated by the Order constitute the entire understanding and agreement between the parties. Each party hereto has read the Contract, understands it and agrees to be bound by its terms and conditions. The Contract supersedes all prior verbal or written agreements between the parties and constitutes the complete and exclusive statement of the terms and conditions between the parties covering the performance hereof.

Appendix B: Removed Prior to Issuance

(page intentionally blank)

Appendix C: Information Security Addendum

Pennsylvania Treasury Department Information Security Addendum

This Information Security Addendum ("Addendum") made as of the Effective Date, by and between the Commonwealth of Pennsylvania, Pennsylvania Treasury Department ("Treasury") and _____ ("Contractor") sets forth additional terms and conditions with respect to information security applicable to _____ (the "Agreement). The terms and conditions agreed to in this Addendum are the minimum required for the Agreement and shall take precedence over any term of the Agreement which attempts to reduce, waive or remove these terms and conditions.

BACKGROUND: Treasury wishes to disclose certain information to Contractor pursuant to the terms of the Agreement, and Contractor is authorized to collect and/or use certain information, pursuant to the terms of the Agreement. The parties have entered into this Addendum to protect the privacy and provide for the security and confidentiality of such information.

NOW THEREFORE, in consideration of the foregoing, and the mutual promises and undertakings hereinafter set forth, and the exchange of information pursuant to the Agreement and this Addendum, the parties agree as follows:

I. Definitions

A. *Authorized Persons*. Authorized Persons include Contractor's employees and subcontractors who have appropriate clearance and a specific need for such access in order to perform Contractor's services for Treasury.

B. *Industry Standards*. Industry Standards include National Institute of Standards and Technology (NIST) 800 Series, NIST Cybersecurity Framework and ISO 27001/2, or their generally recognized equivalents.

C. *Treasury Data*. Treasury Data is any data or information that Contractor creates for Treasury; obtains, accesses, receives from Treasury or on behalf of Treasury; or hosts for or on behalf of Treasury. Treasury Data includes but is not limited to: computer code; Treasury or Commonwealth bank account information; investment account information; identifiers unique to Treasury; and Personally Identifiable Information.

D. *Personally Identifiable Information or PII.* Personally Identifiable Information or PII means information or data, alone or in combination with other information, that identifies or authenticates a particular individual. PII may include, without limitation, name, date of birth, full address (e.g., house number, city, state, and/or zip code), passwords, PINs, biometric data, unique identification numbers (e.g., social security numbers, tax ID numbers, driver license numbers, credit or debit account numbers, medical record numbers), federal or state tax information, TAP/ABLE account numbers, bank account numbers, ACH information, answers to security questions or other personal identifiers, or which meets the definition ascribed to the term "Personal Information" under §6809(4) of the Gramm-Leach-Bliley Act.

E. *Public Data*. Public Data means any specific information or data, regardless of form or format, that Treasury has actively and intentionally disclosed, disseminated, or made available to the public. No Contractor shall make a determination on Treasury's behalf whether data is public or would be

considered public under state or federal law including the Pennsylvania Right-to-Know Law.

F. *Multi-Factor Authentication*. Multi-Factor Authentication is the use of two or more of the Authentication Methods listed below. Two-factor would employ two of the methods; three-factor would employ one each of all three methods.

i. Something you know (e.g., PIN, password, shared information)

ii. Something you possess (e.g., token, smart card, digital certificate)

iii. Something you are (biometrics – e.g., fingerprint, voice, iris, face).

G. *Services*. Services are the services pursuant to the Agreement and/or any Statement of Work ("SOW") or any subsequent document that may detail services.

H. *Documentation*. Documentation means all technical and user documentation provided by Contractor and any succeeding changes thereto, including, without limitation, all specifications; installation, maintenance, operating and customer manuals, instructions and diagnostics; system administrative materials; configuration guides; product guides; and other documentation provided by Contractor related to the Services.

I. *Treasury Confidential Information*. Treasury Confidential Information means Treasury Data that is not Public Data, including but not limited to information containing Personally Identifiable Information, protected health information ("PHI") and electronic protected health information ("ePHI") as defined in HIPPA regulations, investment portfolio information and trade secrets.

II. Assignment.

Contractor may not assign, in whole or in part, this Agreement or Addendum or its rights, duties, obligations, or responsibilities hereunder without the prior written consent of the Treasury. Such consent may be withheld at the sole and absolute discretion of the Treasury.

III. Software/Platform/Website.

a. Software. If Contractor at any time during the term of the Agreement, or during the term of any applicable license or subscription for any software under the Agreement, becomes aware of any Disabling Device in or affecting any product(s) or other items acquired by Treasury from Contractor, or a security flaw in any such software, or a flaw in such software that has the potential to cause or result in a security breach, then the Contractor shall notify Treasury within 72 hours thereafter. Any Contractor notice to Treasury shall include notifying Treasury if it has a fix for the issue, if it is working on a fix, or if it does not have a fix. Contractor shall use reasonable commercial efforts to cure or correct any such security flaw as soon as practicable. Nothing herein will limit Contractor's indemnification obligations under the Agreement or this Addendum.

b. Platform and Website. Contractor further represents and warrants that it will take appropriate and reasonable precautions, using commercial grade anti-virus and malware recognition programs, to screen any software provided to Treasury, and the platform and any websites owned or operated by Contractor to conduct, market or

promote its activities under this Agreement, for viruses and other malware, and to cause the Contractor's services, any such platform and websites to be made available to Treasury and any other Commonwealth agency free of any Disabling Devices (as defined below) or other malware. For purposes of this Addendum, "Disabling Device" means any malware or other computer code (i) that is designed to disrupt, disable, harm, or otherwise impede in any manner the operation of any software program or code, or any computer system or network (commonly referred to as "malware", " spyware", "viruses" or "worms"); (ii) that would disable or impair the operation thereof or of any software, computer system or network in any way based on the elapsing of a period of time or the advancement to a particular date or other numeral (referred to as "time bombs", " time locks", or "drop dead" devices); (iii) that is designed to or could reasonably be used to permit Contractor or any third party to access any computer system or network (referred to as "trojans", "traps", "access codes" or "trap door" devices); or (iv) that is designed to or could reasonably be used to permit Contractor or any third party to track, monitor or otherwise report the operation and use of any software program or any computer system or network by Treasury, its contractors or third parties, in a manner other than in accordance with the specifications and Documentation therefor provided by Contractor or required under applicable law or regulatory rules or requirements. Notwithstanding the foregoing, any code included or used by Contractor as part of the Contractor's services for the sole purpose of allowing Contractor to perform its obligations under this Agreement, or for operational and quality control purposes in connection with such performance, will not be considered a Disabling Device.

c. Data Security.

i. Industry Standards. The Contractor shall ensure that Services procured under this Agreement comply with the applicable Industry Standards. In the event such standards change during Contractor's performance, and the Commonwealth requests that Contractor comply with the changed standard, then any incremental costs incurred by Contractor to comply with such changes shall be paid for pursuant to a change order to the Agreement.

ii. Data Protection. To the extent that Contractor is charged with creating, accessing, transmitting, maintaining, hosting or using Treasury Data under the Agreement, Contractor shall preserve the confidentiality, integrity and availability of Treasury Data by implementing and maintaining administrative, technical and physical controls that conform to Industry Standards. Implemented security controls shall provide a level of security which is commensurate with the sensitivity of the data to be protected.

iii. Data Use and Access. Contractor shall use Treasury Data only and exclusively to support the performance of Services for Treasury under the Agreement and not for any other purpose. With the exception of Public Data, absent Treasury's prior written consent, Contractor shall not at any time during or after the term of the Agreement disclose Treasury Data to any person, other than Authorized Persons and Treasury personnel in connection with the performance of the Services (except as required by law). If such disclosure is required by law, Contractor shall limit such disclosure to information required to be disclosed and shall notify Treasury as soon as practicable and prior to such disclosure, unless such notification is prohibited by law.

iv. Data Backup. Where appropriate to protect the integrity and availability of Treasury Data, Contractor shall maintain (and cause any third-party hosting company that it uses to maintain) a means to backup and recover Treasury Data in the event that Treasury Data is lost, corrupted or improperly destroyed. Treasury shall have the right to establish its own backup security for Treasury Data and to keep such backup Treasury Data and Treasury Data files in its possession if it chooses. Contractor shall cooperate with Treasury in facilitating the establishment and maintenance of such alternative backup security. At no time may Contractor store Treasury Data outside of the United States.

v. Return of Treasury Data. Contractor shall ensure that, upon request, Treasury can access and retrieve Treasury Data in the event the Contractor is unable to continue providing the Services under the Agreement due to termination of the Agreement or otherwise. In the event of a termination for any reason and upon Treasury's request, the Contractor will provide Treasury Data in a standard format or other mutually acceptable format. Treasury will reimburse Contractor for any costs incurred by Contractor to provide Treasury Data in a non-standard format.

vi. Destruction of Treasury Data. Upon written request of Treasury, Contractor shall irrevocably erase or destroy in such a manner to render unrecoverable all Treasury Data in Contractor's possession that is no longer required for the performance of its duties under the Agreement. Upon Treasury's request, Contractor shall certify in writing that these actions have been completed within seven (7) days of Treasury's request.

vii. Effect of Termination. Unless directed otherwise by Treasury, upon termination of the Agreement for any reason, Contractor shall maintain Treasury Data and continue to extend the protections of the Agreement and this Addendum to such information for a period of six months at which point it shall return (or at Treasury's request destroy) all Treasury Data received from Treasury (or created or received by Contractor on behalf of Treasury) regardless of form, and shall retain no copies of Treasury Data except as required by law. If return or destruction of all Treasury Data is not feasible, or any Treasury Data is required to be retained by Contractor under applicable law, Contractor shall continue to extend the protections of the Agreement and this Addendum to such information and limit further use of Treasury Data to those purposes that make the return or destruction of Treasury Data infeasible.

d. Contractor Security.

i. Information Security Program. For the term of the Agreement, Contractor agrees that it has and will maintain a formal information security program which is appropriate for the types of services that it provides. Treasury has adopted the Minimum Security Requirements set forth below (Parts (IV) through (XIII)) in order to outline the security requirements which apply to all third parties, service providers, processors, and contractors (including Contractor) (collectively, "Third Parties") that process Treasury Confidential Information or who have access to Treasury systems. Treasury has identified ISO 27001 Control Requirements; however, Third Parties may identify and rely upon other controls which meet the essence of the requirements.

ii. Contractor Personnel. Contractor agrees that it shall only use highly qualified and appropriately skilled and experienced personnel and contractors in

performing the Agreement and, to the extent not prohibited by applicable law, shall require each to pass a background check.

iii. Acceptance of Acceptable Use Policy. Contractor shall ensure that all Contractor personnel, including employees and contractors, who access Treasury's network as a part of performing the Agreement, will agree to Treasury's Acceptable Use Policy as found in Management Directive 205.34, as it may be amended from time to time.

iv. Multi-Factor Authentication. For services exposed to the Internet, where sensitive information is stored, processed or transmitted, Contractor will provide Multi-Factor Authentication for user authentication to the web application via workstation and mobile browsers. If the service is provided via mobile application as well, that application must also be protected by Multi-Factor Authentication.

v. Security Awareness Training. Contractor shall ensure its personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with Commonwealth of Pennsylvania IT Policies. A comprehensive compilation of these policies can be found at https://www.oa.pa.gov/Policies/Pages/itp.aspx or by visiting the Pennsylvania Office of Administration's website and toggling to IT Policies under the "Policies."

e. Security Incident and Breach Notification.

i. Contractor agrees to notify Treasury upon learning of: (i) unauthorized access, loss, alteration, theft or corruption of Treasury's Confidential Information; (ii) any event that creates a substantial risk to the confidentiality, integrity or availability of Treasury Data; (iii) a breach of any of Contractor's security obligations under this Addendum; or (iv) any other event requiring notification under applicable law. In such an instance, Contractor agrees to:

a) Take such action as may be necessary to preserve forensic evidence and eliminate the cause of the risk or breach within Contractor's reasonable control. As soon as practicable after discovery, Contractor shall undertake a thorough forensic investigation of any compromise or improper use and provide Treasury all information necessary to enable Treasury to fully understand the nature and extent of the compromise or improper use to the extent known;

b) Notify Treasury by telephone at (717) 787-8726 and (717) 705-6428 and by e-mail at ITSecurity@patreasury.gov regarding such an event without undue delay and in any event within 24 hours of discovery; and

c) To the extent that the breach or incident was caused by Contractor's failure to comply with the requirements of the Agreement or this Addendum, or otherwise was caused by the fault of Contractor, assume the cost of informing all such affected individuals in accordance with applicable law, in addition to its other indemnification obligations under this Addendum.

ii. Security Incident Investigations.

Contractor agrees to cooperate with Treasury in investigating a security incident, as notified by Contractor under this Addendum or declared by Treasury, and provide the name and contact information, of at least two (2) security contacts who will respond to Treasury in a timely manner, dependent on criticality, in the event that Treasury must investigate a security incident. The current security contacts are as follows:
Contact Names: _____ _____
Phone Numbers: _____ _____
Email Addresses: _____ _____

f. Maintenance of Safeguards.

i. Contractor shall maintain and follow Industry Standards with respect to any of Treasury's Confidential Information in Contractor's possession or control and protect such information against any loss, alteration, theft or corruption.

ii. At Treasury's request, Contractor shall provide Treasury with copies of its information security policies, processes, and procedures made available by Contractor to third parties or otherwise requested by Treasury, subject to Contractor's reasonable requirements and restrictions to protect the security and confidentiality of such information. Contractor will notify Treasury of any changes to its policies, processes or procedures that relate to the security of Treasury's Confidential Information in Contractor's possession.

g. Information Security Audit.

i. Treasury shall have the right to review Contractor's information security program prior to the commencement of Services and from time to time during the Term of the Agreement. During the performance of the Services, on an ongoing basis annually and immediately in the event of a security incident, Treasury, including its professional advisors and auditors, at its own expense, shall be entitled to perform, or to have performed, an on-site assessment of Contractor's information security program.

ii. Treasury shall have the right to review Contractor's information security program through Contractor's annual submission to Treasury of its current SOC2 report. The report must document an assessment conducted by a qualified, independent third party. Assessment scope must address the services provided to Treasury, including but not limited to related people, processes and technology.

iii. Upon Treasury's request, Contractor agrees to complete, within forty-five (45 days) of receipt of Treasury's request, an assessment questionnaire provided by Treasury regarding Contractor's information security program, including artifacts for a subset of controls.

h. Application Security.

In the event the Contractor conducts application software development for Treasury, Contractor will either make source code available for review by Treasury or will conduct source code scanning using a commercial security tool. Scans must be conducted annually and at any time significant code changes are made. Scan reports will be made available to Treasury within two weeks of execution. Contractor must disclose remediation timelines for high, medium and low risk security code defects. Scans must occur before code is implemented in production. High risk security code defects may not be implemented in production without written approval from Treasury's Chief Information Officer. Contractor shall not deliver any code that

provides for back door access or otherwise would constitute a Disabling Device under this Addendum, except as specified and approved by Treasury. Contractor shall comply with the software development security requirements identified under Part (VII) below and inform Treasury of any code development internal requirements, procedures and/or policies that Contractor uses to establish and verify the quality and security of Contractor's code development services.

i. Compliance with Applicable State and Federal Law.

Contractor shall comply with all applicable federal, state, and local laws concerning data protection and privacy when performing the Services and storing, handling or transmitting Treasury Data.

j. Enforcing Compliance.

Contractor shall enforce and be responsible for compliance by all its personnel and contractors with the provisions of this Information Security Addendum and all other confidentiality obligations owed to Treasury.

k. Accommodation of Additional Protections.

Contractor agrees to comply with such additional protections as Treasury shall reasonably request.

l. Termination.

A breach by Contractor of any provision of this Addendum, as reasonably determined by Treasury, shall constitute a material breach of the Agreement and shall provide grounds for immediate termination of the Agreement by Treasury pursuant to the Agreement.

m. Indemnification.

Contractor shall indemnify, hold harmless and defend Treasury from and against all claims, losses, liabilities, damages, judgments, costs and other expenses, including Treasury's costs and attorney fees, incurred as a result of, or arising directly or indirectly out of or in connection with (i) Contractor's failure to meet any of its obligations under this Addendum; (ii) any security breach or incident that was caused by Contractor's failure to comply with the requirements of the Agreement or this Addendum, or otherwise was caused by the fault of Contractor; and (iii) any claims, demands, awards, judgments, actions and proceedings made by any person or organization arising out of or in any way connected with Contractor's performance under this Addendum. Limitations on Contractor's liability, regardless of conflicting language elsewhere in the Agreement, shall not apply to claims related to Contractor's breach of the requirements of this Addendum.

n. Intellectual Property Infringement Indemnification.

Contractor shall indemnify, defend and hold Treasury harmless from any and all claims brought against Treasury alleging that the Services and/or Documentation or Treasury's use of the Services and/or Documentation, or use of any deliverables provided by Contractor, constitutes a misappropriation or infringement of intellectual property ("IP") of any Third Party. Contractor agrees to be responsible for all costs or expenses, to include reasonable attorneys' fees awarded or resulting from any claim. Treasury shall, after receiving notice of a claim, advise Contractor of such notification. Limitations on Contractor's liability, regardless of conflicting language elsewhere in any Agreement, shall not apply to claims related to Contractor's misappropriation or infringement of another's intellectual property.

o. Contractor Liability Insurance.

Treasury may require Contractor to procure, and maintain for the duration of the Agreement and a specified period thereafter, insurance against claims and damages which may arise from or in connection with the performance of its work to include IP infringement, professional liability, cybersecurity, and privacy or data breach coverage, with coverage amounts reasonably acceptable to Treasury.

p. Survival; Order of Precedence.

The provisions of this Addendum shall survive expiration or termination of the Agreement.

q. Entire Agreement.

The Agreement, including any exhibits and/or schedules thereto, and this Addendum contain the entire understanding of the parties with respect to the subject matter hereof and supersedes all prior agreements, oral or written, and all other communications between the parties relating to such subject matter.

IV. Minimum Security Requirements

The below requirements apply to all Third Parties (including Contractor) that process Treasury Confidential Information or PII on behalf of Treasury, or if they have a direct connection to the Treasury network. While ISO 27001 controls are listed, equivalent controls from other frameworks may be used in accordance with those frameworks, if they meet the essence of the requirement.

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
5.1.1	Policies for information security	A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.
5.1.2	Review of the policies for information security	The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
6.1.1	Information security roles and responsibilities	All information security responsibilities should be defined and allocated.
7.2.2	Information Security Awareness, Education and Training	All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
8.1.1	Inventory of Assets	Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.
8.1.4	Return of Assets	All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement.
9.1.2	Access to Networks and Network Services	Users should only be provided with access to the network and network services that they have been specifically authorized to use.

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
9.2.1	User Registration and De-Registration	A formal user registration and de-registration process should be implemented to enable assignment of access rights.
9.2.2	User Access Provisioning	A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.
9.2.3	Management of Privileged Access Rights	The allocation and use of privileged access rights should be restricted and controlled.
9.2.6	Removal or Adjustment of Access Rights	The access rights of all employees and external party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.
9.4.1	Information Access Restriction	Access to information and application system functions should be restricted in accordance with the access control policy.
9.4.2	Secure Log-On Procedures	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.
9.4.3	Password Management System	Password management systems should be interactive and should ensure quality passwords.
10.1.1	Policy on the Use of Cryptographic Controls	A policy on the use of cryptographic controls for protection of information should be developed and implemented.
11.1.1	Physical Security Perimeter	Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
11.1.2	Physical Entry Controls	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
11.1.3	Securing Offices, Rooms and Facilities	Physical security for offices, rooms and facilities should be designed and applied.
11.1.4	Protecting Against External and Environmental Threats	Physical protection against natural disasters, malicious attack or accidents should be designed and applied.
12.1.4	Separation of Development, Testing and Operational Environments	Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.
12.2.1	Controls Against Malware	Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.
12.4.1	Event Logging	Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.
12.4.3	Administrator and Operator Logs	System administrator and system operator activities should be logged, and the logs protected and regularly reviewed.

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
12.6.1	Management of Technical Vulnerabilities	Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
13.1.1	Network Controls	Networks should be managed and controlled to protect information in systems and applications.
13.1.3	Segregation in Networks	Information involved in electronic messaging should be appropriately protected.
14.1.3	Protecting Application Services Transactions	Information involved in application service transactions should be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
14.3.1	Protection of Test Data	Test data should be selected carefully, protected and controlled.
15.1.1	Information Security Policy for Supplier Relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented.
15.2.1	Monitoring and Review of Supplier Services	Organizations should regularly monitor, review and audit supplier service delivery.
15.2.2	Managing Changes to Supplier Services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and reassessment of risks.
16.1.5	Response to Information Security Incidents	Information security incidents should be responded to in accordance with the documented procedures.
18.2.1	Independent Review of Information Security	The organization's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur.
Network and system vulnerability assessments shall be conducted on an annual basis, at a minimum. Critical vulnerabilities shall be tracked and remediated within 30 days of identification.		
Additional Requirements		
Local accounts shall be disabled if not required or used and shall not be used for privileged access.		
Third party shall notify Treasury of any separation or transfer of Third-Party Worker with Treasury credentials no later than the day of that event.		
Accounts shall be disabled after 90 days of inactivity, at a minimum.		
Treasury Confidential Information shall not be processed or stored on personal accounts or on personally owned computers, devices or media.		
Third-Party shall notify Treasury within a reasonable period, in no event to exceed five (5) business days after discovery, or shorter if required by applicable law or regulation, of any potential Cybersecurity Vulnerability. Third-party shall report all critical Cybersecurity		

<table>
<tr><th colspan="3">ISO 27001 Control Requirements</th></tr>
<tr><th>ISO Control Ref</th><th>Control Objective</th><th>Control Description</th></tr>
<tr><td colspan="3">Vulnerability that would have a significant adverse effect on Treasury and any Cybersecurity Vulnerability to Treasury at ITSecurity@patreasury.gov</td></tr>
<tr><th colspan="3">Security Incident Notification Requirements</th></tr>
<tr><td colspan="3">Third Party shall implement and maintain a written Incident Response Plan containing policies and procedures sufficient to comply with its breach notification obligations under this Agreement and applicable data protection and privacy Laws.</td></tr>
<tr><td colspan="3">Notification and Cooperation. Third Party shall:
Provide Treasury with the name and contact information for any employee of Third Party who shall serve as the Treasury's primary security contact and shall be available to assist Treasury twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a Security Incident;
Notify Treasury and Treasury's primary business contact within Third Party of a Security Incident as soon as practicable, but no later than twenty-four (24) hours after Third Party becomes aware of the Security Incident. Immediately following Third Party's notification to Treasury of a Security Incident, the parties shall coordinate with each other to investigate the Security Incident. Third Party agrees to fully cooperate with Treasury in the investigation of any Security Incident, including without limitation, by assisting with any investigation, making available all relevant records, logs, files, data reporting and other materials helpful to the investigation, and providing reasonable access to Third Party's facilities, systems, and personnel;
Maintain and preserve all documents, records and other data related to the Security Incident;
Fully cooperate, at its own expense, with Treasury in any litigation, investigation or other action deemed reasonably necessary by Treasury to protect its rights related to the Security Incident; and
Use its best efforts to prevent a recurrence of any such Security Incident.</td></tr>
<tr><td colspan="3">Expenses of Remediation. Third Party shall, at its own expense, use best efforts to immediately contain and remedy any Security Incident and prevent any further Security Incident, including, but not limited to, taking any and all action necessary to comply with Applicable Law. Third Party shall reimburse Treasury for all actual costs incurred by Treasury in responding to and mitigating damages caused by any Security Incident, including all costs of notice to third parties and remediation pursuant to the following section, including, but not limited to, costs incurred by Treasury relating to forensic investigators, legal counsel, telephone call centers, notification vendors, and business disruption.</td></tr>
<tr><td colspan="3">Disclosure to Third Parties. Third Party agrees that it shall not inform any third party of any Security Incident without first obtaining Treasury's prior written consent, other than to inform a complainant that the matter has been forwarded to Treasury's legal counsel. Further, Third Party agrees that Treasury shall have the sole right to determine: (i) whether notice of the Security Incident is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in Treasury's discretion; and (ii) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.</td></tr>
</table>

V. Physical Security Requirements

In addition to the Minimum Security Requirements regarding Physical Security defined above (11.1.1 – 11.1.4), the below requirements apply to all Third Parties (including Contractor) that process, access, or store (physically or logically) Treasury Confidential Information or PII on behalf of Treasury, or if they have a direct connection to the Treasury network. If Treasury data is only stored or processed in a cloud environment, the identified cloud provider must be communicated to Treasury and the associated attestation reports (SOC 2 Type 1 & 2 Report, ISO 27001/2) must be provided to Treasury.

Physical Security Control Requirements
For all facilities used to access, process, transmit, and/or store Treasury Confidential Information or Personal Information, badge readers shall be used on all entry points to ensure physical access is restricted to authorized personnel.
All servers and network equipment used to store and/or access Treasury Confidential Information or Personal Information shall be kept in a secure room with the following controls: 1. Additional access control mechanisms (e.g., badge, biometrics, pin, etc.) on entry doors, 2. Rooms are located on the interior of the building with no windows, unless safeguards are in place to prevent shattering, and 3. Telecommunications equipment, cabling and relays receiving data or supporting services are hidden from view to deter interception or damage.
For all facilities used to access, process, transmit, and/or store Treasury Confidential Information or Personal Information, security cameras shall be implemented to monitor the perimeter, entry/exit points, and the interior of the facility.
Security camera recordings shall be retained for at least 30 days.
For all facilities used to access, process, transmit, and/or store Treasury Confidential Information or Personal Information, access shall be controlled by a security guard, mantrap, or other means when entering the facility.
Identification badges shall be issued to all employees, contractors, and visitors and worn always.
Identification badges shall delineate full time employees from contractors and visitors.
All physical documents that contain Treasury Confidential Information or Personal Information shall be kept in a locked office, cabinet, or other location which is locked, and access restricted to authorized personnel only.
Mechanisms shall be in place to notify, investigate, and address potential physical security incidents such as physical intrusion or a stolen asset.
If all facilities used to access, process, transmit, and/or store Treasury Confidential Information or Personal Information are not staffed 24x7x365, alarms shall be installed for off-hour access monitoring.
If facilities used to access, process, transmit, and/or store Treasury Confidential Information or Personal Information are shared with other occupants (e.g. co-located data center), protective mechanisms must be implemented between occupants to prevent unauthorized access to your organization's physical equipment (e.g. locked cage, badge access, etc.)
Physical access rights shall be reviewed on an annual basis (at a minimum) and updated as needed to ensure physical access to all facilities used to access, process, transmit, and/or store Treasury Confidential Information or Personal Information is restricted to authorized personnel.

VI. Security Requirements When Processing Sensitive / Regulated Data

In addition to the Minimum Security Requirements defined above, the below requirements apply to all Third Parties (including Contractor) that process Treasury PII), Sensitive

Personal Information (SPI), Protected Health Information (PHI), Payment Card Information (PCI), Intellectual Property (IP) or supports Treasury mission critical business functions:

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
6.1.2	Segregation of duties	Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
7.1.1	Screening	Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
7.2.1	Management responsibilities	Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.
8.3.1	Management of removable media	Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
8.3.2	Disposal of media	Media should be disposed of securely when no longer required, using formal procedures.
8.3.3	Physical media transfer	Media containing information should be protected against unauthorized access, misuse or corruption during transportation.
9.2.4	Management of secret authentication information of users	The allocation of secret authentication information should be controlled through a formal management process.
9.2.5	Review of user access rights	Asset owners should review users' access rights at regular intervals.
9.4.5	Access control to program source code	Access to program source code should be restricted.
11.2.7	Secure disposal or re-use of equipment	All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
12.1.1	Documented operating procedures	Operating procedures should be documented and made available to all users who need them.

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
12.1.2	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled.
12.4.2	Protection of log information	Logging facilities and log information should be protected against tampering and unauthorized access.
12.5.1	Installation of software on operational systems	Procedures should be implemented to control the installation of software on operational systems.
12.6.2	Restrictions on software installation	Rules governing the installation of software by users should be established and implemented.
12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes.
14.2.2	System change control procedures	Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.
16.1.1	Responsibilities and procedures	Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.
16.1.2	Reporting information security events	Information security events should be reported through appropriate management channels as quickly as possible.
16.1.4	Assessment of and decision on information security events	Information security events should be assessed, and it should be decided if they are to be classified as information security incidents.
16.1.6	Learning from information security incidents	Knowledge gained from analyzing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.
18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable.

VII. Third Party Software Development

In addition to the Minimum Security Requirements defined above, the below requirements apply to all Third Parties (including Contractor) that develop software specific to Treasury's needs or host applications that Process Treasury Confidential Information or PII with no Trusted Third-Party Network connectivity to Treasury:

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
14.2.1	Secure development policy	Rules for the development of software and systems should be established and applied to developments within the organization.
14.2.6	Secure development environment	Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
14.2.7	Outsourced development	The organization should supervise and monitor the activity of outsourced system development.
14.2.8	System security testing	Testing of security functionality should be carried out during development.
14.2.9	System acceptance testing	Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.
Additional Requirements		
Third Party may not use offshore developers or outsourced developers without the written approval of the Treasury Chief Information Security Officer.		
Third Party shall provide all developers application security training.		
All confirmed critical/high vulnerabilities (mediums and low depending on impact) found during testing shall be remediated and retested within 30 days of identification and prior to moving code to production. A formal report including the scope and results of security testing (including any issues/exceptions) shall be provided to Treasury upon request.		
Any software developed for Treasury shall not contain any software (proprietary or open source) developed or sold by an entity other than Third Party unless approved by Treasury.		
All software delivered to Treasury shall be free of defects/vulnerabilities identified as "critical" or "high" risk. If software shall be delivered with critical or high-risk vulnerabilities, approval from the Treasury business application owner shall be obtained.		
Information security checkpoints shall be incorporated into the software development lifecycle including, but not limited to: • Risk assessment process • Documented security requirements • Secure coding guidelines and checklists • Secure design/architecture review • Source code review • Security testing		
If the Third-Party hosted application undergoes significant changes or enhancements, Treasury has the option to perform a technical penetration test (manual and/or automated) prior to the changes being implemented in production. In cases deemed acceptable by Treasury, a Third		

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
Party's penetration test results shall be leveraged if the report meets Treasury's quality standards and was conducted within the last 12 months.		
All Third-Party hosted applications shall be reassessed every two years. Reassessment includes but is not limited to a technical penetration test (manual and/or automated).		
Third Party Software Developer with Trusted Network Connectivity to Treasury		
Third Party shall have a designated application security representative that acts as the primary liaison between Third Party and Treasury in matters related to secure application development, ensuring that Third Party development teams meet all Treasury requirements for secure application development, and provides to Treasury, upon request, evidence of compliance with requirements listed in this section.		
Prior to the initiation of any project, Third Party shall request the application's risk classification (Critical vs. non-Critical) and network exposure designation (External or Internal facing) from the Treasury application owner. These risk factors shall be determined prior to the initiation of code development.		
Documented security requirements shall be formally defined for all new development of applications including projects involving significant changes to existing applications with the Treasury designation of "Critical" and/or "External facing". These requirements shall be developed in collaboration with the Treasury application owner and other key stakeholders as necessary. All secure design requirements shall be documented and maintained with the broader set of application requirements.		
Software development teams shall use Treasury-provided version control processes and tools.		
Application development shall take place in a secured development environment. The development environment shall incorporate the following controls: Access Control, Offsite backup, Logical separation between different development environments (e.g. development, staging, testing, etc.), change control for associated systems supporting development environments, approval process for code changes of the application prior to production release, specific permissions and logging of approvals associated with movement of code and test data into and out of the environment.		

VIII. Cloud Security

In addition to the Minimum Security Requirements defined above, the below requirements apply to all Third Parties (including Contractor) that host a cloud computing application (in a SaaS, PaaS, IaaS, or DRaaS environment) that Processes Treasury Confidential Information or PII), or the Third Party provides a cloud computing platform that allows Treasury to develop, run, and manage applications, or the Third Party is responsible for the management of virtual machine image and/or hypervisor on behalf of Treasury:

Cloud Security Requirements
Root/administrator access to the management console shall require multi-factor authentication.
Dedicated secure networks shall be separate from customer production infrastructure, leveraged to provide management access to the cloud infrastructure.
Third Party shall have the ability to provide logs which are specific to the instances used for Treasury or the Treasury engagement.
Third Party shall enable console and resource level logging across regions in the cloud infrastructure.
All logs in the cloud environment shall feed into a central log aggregation tool.

Third Party shall regularly back up application configuration, data within the application, database and configuration of systems within cloud infrastructure to ensure that data can be restored if needed.
Third Party shall retain the original structure and format of data residing within the cloud application for easy movement to another cloud solution / cloud service provider.
Third Party shall support federated authentication (e.g.: SAML) or standards-based identity protocols (e.g., OpenID Connect, OAuth2, etc.) leveraged for propagating and enforcing identity controls through the SaaS and API.
Third Party shall have cryptographic controls implemented to make sure that Treasury data at rest within cloud infrastructure is always encrypted (e.g.: AES-256).
Third Party shall have mechanisms in place to control encryption key generation, distribution, storage, access and destruction.
Third Party shall have access to management consoles and cloud application(s) restricted through Role Based Access Control & based on the least privilege principle.
If keys (e.g.: access key, secret key for cloud accounts or SSH keys used for managing cloud instances) are used for managing the cloud infrastructure; the Third Party shall keep in a protected vault with access controls.
Third Party shall have a cyber incident management program in place wherein the cyber events/incidents are evaluated, contained, remediated, and responded to.
Third Party shall have a patch management process for identifying and applying all relevant vendor patches and security updates within 30 days of release by vendor.
Third Party shall have the root/administrator account credentials vaulted.
A web application vulnerability assessment or penetration test shall be performed on the cloud application(s) hosting, storing, processing and/or transmitting Treasury data, in the last 12 months.
A network vulnerability assessment shall be performed on the cloud instances and systems (servers, databases, networking components/devices) which store, process, host, or transmit Treasury data within the last 12 months.
Third Party shall have application support for both single tenancy and multi-tenancy deployment.
Third Party shall support web application firewall (WAF) implementations which comply at minimum with the OWASP top 10 risks.
Third Party shall have controls in place to ensure non-public exposure of data, including but not limited to S3 buckets and Elasticsearch.
Third Party shall have audits to monitor for configuration drift.
Third Party shall have controls to automatically shut down publicly exposed data.

IX. Software as a Service (Saas) Security

In addition to the Minimum Security Requirements and the Cloud Security Requirements defined above, the below requirements apply to all Third Parties (including Contractor) that hosts a cloud computing application that Processes Treasury Confidential Information or PII on behalf of Treasury:

SaaS Security Requirements
SaaS provider is accountable for maintaining compliance with relevant regulations and legal requirements for its services.
SaaS provider shall provide documentation to tenants regarding the following: • Roles and responsibilities matrix between cloud service provider and Treasury for each platform/service offering (e.g., incident response, infrastructure support, access

management, etc.). Methods for maintaining segregation of duties within the cloud service offering shall also be included. • Scenarios in which the cloud service provider may access tenant data and metadata. • Installation, configuration, and use of products/services/features. • Known issues with products/services of the cloud offering. • Transport routes of data between systems and governing procedures for data migration to and from cloud service offering(s). • How system (e.g., network, storage, memory, I/O, etc.) oversubscription is maintained and under what circumstances/scenarios. • List of Third Parties (sub processors or joint controllers) that have access to Treasury Confidential Information or manage aspects of the application, database, server operating system, etc.
Configuration of the SaaS shall adhere to a minimum baseline of security configuration settings for role, scope and location of the services.
SaaS provider that directly provides services to Treasury is solely accountable for the platform and infrastructure security. If the provider uses other cloud or Third-Party service vendors, the provider is accountable for ensuring the security arrangement meets Treasury contractual requirements.
Integration of the SaaS with Treasury resources shall leverage Treasury pre-approved integration architecture pattern(s).
All service endpoints shall be signed by a trust authority or there must be another mechanism of establishing trust available.
SaaS provider shall ensure data portability among different cloud services by supporting standardized file format, import/export functionality, etc.
SaaS provider shall support standard based identity protocols and enforcement such as OpenID Connect (OIDC), Security Assertion Markup Language (SAML) and OAuth2 for propagating and enforcing identity controls through SaaS and Application Programing Interfaces (API).
SaaS provider shall have the capability to support tenant-generated and stored encryption keys.
Access to management consoles for entitlement and policy management shall be secure and restricted through Role Based Access Control (RBAC) and be based on the least privilege principle. Credential(s) for privileged accounts, including root or administrator accounts, shall be vaulted and multi factor authentication shall be implemented.
Upon request, SaaS provider shall inform Treasury of application user access that has been provisioned and de-provisioned for the Treasury account.
SaaS provider shall have the capability to provide secure data disposal at Treasury's request and ensure data is not recoverable by any computer forensic means.
SaaS provider shall triage threats and security related events in multi-tenant environments on a global scale and ensure timely and thorough incident management.
SaaS providers shall demonstrate compliance with information security and confidentiality, service definitions, and service level agreements. SaaS provider reports, records, and services shall undergo audit and review at planned intervals to govern and maintain compliance with the service delivery agreements.
SaaS provider shall use dedicated secure networks to provide management access to cloud service infrastructure that is separate from the customer (tenant) production infrastructure.
SaaS provider shall permit tenants to perform independent vulnerability assessments of the customer (tenant) production infrastructure.
SaaS provider shall allow tenants to opt-out of having their data/metadata accessed via inspection technologies.
SaaS provider shall have an option for customers to opt-in or opt-out of specific features in SaaS releases.

SaaS provider shall have the capability to logically segment and recover data for a specific customer in the case of a failure or data loss.
SaaS provider logging and monitoring framework shall allow isolation of an incident to specific tenants. Upon request, SaaS provider shall provide Treasury with platform management logs, application logs, API activity logs.
Upon request, SaaS provider shall have the capability to restrict the storage of Treasury Data to specific countries or geographic locations.
A web application vulnerability assessment or penetration test shall be performed on the cloud application(s) in the last 12 months.

X. Data Center Security

In addition to the Minimum Security Requirements defined above, the below requirements apply to all Third Parties (including Contractor) that provide data center facility services to Treasury:

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents should be designed and applied.
11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
11.2.1	Equipment siting and protection	Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
11.2.2	Supporting utilities	Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.
11.2.4	Equipment maintenance	Equipment should be correctly maintained to ensure its continued availability and integrity.
17.2.1	Availability of information processing facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

Additional Requirements
Data center walls shall be resistant to fire or explosions.
Data centers with glass windows are not allowed unless shatter proof and impact resistant barriers are in place.

Physical data center access rights shall be reviewed at a minimum quarterly using a documented process.
All data centers shall have professionally installed intrusion alarm systems monitored by either a contracted security monitoring service or by members of the local security team within the building. All ingress points shall be alarmed and monitored. The alarm system shall be capable of continuous operation in the event of a loss of power.
Emergency doors shall have audible alarms and display appropriate signage.
Upon entrance to the data center, access shall be restricted to only the areas the person needs access to. Both ingress and egress points shall be controlled and monitored 24x7x365 to minimize tailgating and provide detailed location logging. Logs shall be retained for a minimum one year from time of event or logging, except where prohibited or otherwise required by applicable laws and regulations. Logs relevant to pending or foreseeable litigation, investigation or audit (even when not subject to a formal document retention notice) shall be preserved as directed by Treasury. Visitors shall be escorted or observed at all times.
Closed-Circuit Television (CCTV) systems and appropriate signage shall be in place on the exterior and all datacenter floor entry points. Cameras shall be monitored during operational hours and be retained for a minimum 30 days.
Management of security alarms, entrance control, environmental controls, and CCTV systems shall be physically and logically restricted to staff responsible for these functions.
All entrances of the building containing the data center shall be designed to block entering the building interior or boarding elevators without first undergoing a manned identification check. The main entrance accessible to the public shall be manned 24/7. Multiple secured entrances shall exist between public and data center floor area.
Assets containing Treasury Confidential Information shall be caged off physically from the rest of the data center. The cage shall utilize the main security card access control system with multi factor authentication or a controlled key process. Cages shall be real floor to real ceiling to prevent unauthorized entry. Cages shall be designed to prevent intrusion or breach from outside of the cage. Finally, cages shall have a camera covering the entrance and be wired into the internal 24x7x365 CCTV system.
Anyone requiring badge access to any computer room shall follow a defined procedure approved by the third party including the badge holder's name, badge number, computer room location, reason access is needed, and termination date for a fixed duration. The Third-Party security office shall not configure any badge for computer room access without being authorized by the Third Party or designated team members.
The building exterior shall be periodically checked by scheduled security walk-throughs. Suspicious packages, activities, vehicles and/or people shall be investigated.
Data center parking area shall have physical obstacles in place to reduce risk of vehicle or car bomb penetrating exterior walls.
All data center workers shall be trained in control and storage of combustible materials (including paper and cardboard), and on the correct processes to follow when detecting a fire.
Server rooms shall not be used for storage and shall be clear of all unnecessary equipment and material not in use.
Detective monitoring and controls shall be implemented to mitigate the risk of overhead water sources impacting the IT equipment. Water detection shall be placed near air conditioners and any other water sources at the lowest level of the room.
Multiple methods of early fire detection shall be implemented and monitored 24X7x365 including smoke and temperature detection.
All data centers shall have a fire suppression system.
Loading bays and docks shall have CCTV coverage that provides a clear head-on view of the vehicle. This view shall be positioned to enable recognition of the driver, make of vehicle and registration number plate. The doors from the holding area into the data center shall conform

to the interior security requirements for entrance to the data center. The movement, delivery or removal of any material or equipment into and out of the facility shall be recorded.
All switches and/or controls, which permit emergency shutdown of vital systems, shall have physical protection, audible alarm and signage to avoid accidental activation.
Third Party shall ensure that all computer devices are connected to surge protectors to protect them against spikes and surges in the electrical power supply.
Third Party shall ensure that backup power supply is available in the form of local generator(s).
Third Party shall ensure that all electrical and mechanical infrastructures are maintained per manufacturer specifications.
Emergency lighting, powered by a supply other than the main power, shall be implemented throughout the data center in accordance with local fire and health and safety regulations. Emergency lighting shall be activated when the fire alarm is raised, or when a degradation of power prevents the standard lights from operating.
The data center shall have systems in place to control and monitor temperature and humidity, air conditioning system to control air quality and minimize contamination. Server room temperature shall be controlled and monitored. Server room humidity shall be controlled and monitored within the range of 40-60% relative humidity.
The data center shall have air conditioning systems with separate zones for standard working areas, and areas containing equipment such as server rooms.
The air conditioning system supporting server rooms shall have dust filtration systems in place and shall be reviewed periodically to ensure air quality does not degrade / contamination increases.
Server rooms shall have positive pressurization to minimize contaminants entering these areas.
A process shall be in place for scheduled testing and maintenance of all critical data center infrastructure including security, power and environmental systems. Repairs or modification to facility security components (e.g., doors, locks, walls, hardware) shall be documented.
Critical data center infrastructure including power and environmental systems shall be engineered to function through an operational interruption. IT equipment with multiple power supplies shall leverage the redundant power infrastructure.
The data center access control system, and doors, shall be designed to maintain operation during scenarios such as: The failure of the access control application or hardware platform and a utility power outage.
All Treasury equipment shall be properly mounted in appropriately sized racks which are ground and/or ceiling mounted in accordance with local earthquake guidelines. Racks shall be labeled. Equipment in racks as well as cables into racks shall also have labels.
New equipment shall be stored in a secured area. Third Party personnel shall inspect the box for tampering before opening. Movement of used equipment containing Treasury data shall be done under the supervision of third-party personnel via a security approved process.
Third party shall have a documented equipment or media delivery or handling process.
Data centers shall have a disaster recovery plan for the facility and environmental that at least identifies and mitigates risks to Treasury services in the event of a disaster. The plan shall provide for contingencies to restore facility service if a disaster occurs, such as identified alternate data center sites. The plan shall be shared with Treasury to ensure Treasury can coordinate with its own DRP.
Data centers shall conduct an electrical blackout test, at least annually, to validate continue functionality through an operational interruption. Additionally, the data center shall participate and support Treasury DRP and associated testing.
All Treasury equipment shall be completely network segregated from non-Treasury parts of the data center.

XI. Direct, Trusted, Network Connection to Treasury

In addition to the Minimum Security Requirements defined above, the below requirements apply to all Third Parties (including Contractor) that have a direct, trusted network connection to Treasury:

Direct, Trusted, Network Connection Requirements
Third party shall use only Treasury managed devices or sessions, a Treasury Virtual Private Network (VPN) with two-factor authentication, or Virtual Desktop Infrastructure (VDI) with two-factor authentication to directly connect to Treasury resources.
Treasury conducts periodic scans on all Treasury owned IP addresses. If Treasury notifies the third party of any confirmed high or critical vulnerability found, the third party shall remediate the confirmed vulnerability within 30 days.
Remote access to a trusted Third-Party network is only allowed through the Treasury Virtual Private Network (VPN) with two-factor authentication.

XII. System and Data Availability

In addition to the Minimum Security Requirements defined above, the below requirements apply to all Third Parties (including Contractor) that manage, support, maintain systems or process, access, or store data that has high availability requirements, or the Third Party's service / application has high availability requirements as defined by Treasury:

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
12.1.1	Documented operating procedures	Operating procedures should be documented and made available to all users who need them.
12.1.3	Capacity management	The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
12.3.1	Information backup	Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.
17.1.1	Planning information security continuity	The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g., during a crisis or disaster.
17.1.2	Implementing information security continuity	The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

ISO 27001 Control Requirements		
ISO Control Ref	**Control Objective**	**Control Description**
17.1.3	Verify, review and evaluate information security continuity	The organization should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

Additional Requirements
Third Party shall maintain a Disaster Recovery Plan (DRP) for all locations and applications used to provide services to Treasury. The DRP shall include the following elements: • Documented critical business functions, applications and supporting technologies. • Document what factors trigger a disaster, who is authorized to declare a disaster, and the communication plan, including notification to Treasury. • Identify alternate locations with the necessary infrastructure to support the recovery needs. • Document the management and membership of the disaster response and recovery teams. • Document service level, RTO's and RPO's. • Document the required recovery actions, identify and ensure the availability of required resources, and compile this information as the recovery plan. • Identify critical technology service provider dependencies and recovery support capability.
If Third Party provides a SaaS service, Third Party shall provide Treasury with geographically resilient hosting options. Third Party shall have more than one provider for each service for which there is a service delivery dependency
The disaster recovery plan must be reviewed and signed off every 12 months. Lessons learned should be captured as part of the disaster recovery exercise.
All data retention requirements should be documented and approved by Treasury.

XIII. PaaS Security

In addition to the Minimum Security Requirements and the Cloud Security Requirements defined above, the below requirements apply to all Third Parties (including Contractor) that provide a cloud computing platform to Treasury to develop, run, and manage applications:

PaaS Requirements
Maintain effective policies, guidelines, and processes to govern and control Virtual Machine (VM) lifecycle management, including self-service and automated scripts / DevOps tools.
Control the creation, storage, use, retirement and destruction of VM images with a formal change management process and tools and approve additions only when necessary.
Keep a small number of known-good and timely patched images of a guest operating system separately and use them for fast recovery and restoration of systems to the desired baseline.
Discover virtual systems, including dormant VMs and the applications running on them, regularly.
Use virtualization products with management solutions to examine, patch, and apply security configuration changes to VMs.

Maintain policies to restrict storage of VM images and snapshots. If it is necessary to store images and snapshots, proper authorization, such as secondary level of approval, shall be obtained and corresponding monitoring and control processes shall be established.
Control the backup, archiving, distribution, and restart of VMs with effective policies, guidelines, and processes such as suitably tagging the VM based on sensitivity / risk level.
Create a controlled environment to apply security patches and control policies to an offline or dormant VM.
Regularly monitor virtual appliances that provide critical infrastructure, management, and security services.
Ensure proper hardening and protection of VM instances through VM guest hardening.

PROPOSAL COVER SHEET: RFP25-002 Colocation of Data Center Facility

This cover sheet must be included with your submittals no later than 5PM on Monday June 9th, 2025, to the Issuing Office via email to RFP25-002@patreasury.gov.

If you have any questions, please email RFP25-002@patreasury.gov

Submitted by: (legal name of entity) _____

Authorized Signature: _____ **Date:** _____

Print Name and Title: _____

Address: _____

City/ State/ Zip: _____

Email address: _____ **Telephone No:** _____

This entity is incorporated in: _____

County Located _____ **Federal ID#** _____

This entity is a: (check the applicable option)

- ☐ Corporation
- ☐ General Partnership
- ☐ Limited Liability Company
- ☐ Limited Partnership
- ☐ Unincorporated Association
- ☐ Sole Proprietorship

This entity is claiming status as: o Small Diverse Business o Veteran Business Enterprise and has submitted proper proof as required in Part II of this RFP.

Is the Offeror authorized to transact business in the state of Pennsylvania? _____

Please complete this form. This form and all required submissions must be received no later than **Monday June 9th 2025, 5PM**. Late bids will not be considered regardless of the reason.

Please return your proposals to:
RFP25-002 Issuing Office
via email to RFP25-002@patreasury.gov

COST PROPOSAL

COST PROPOSAL/ADDITIONAL INFORMATION - Please complete the cost proposal utilizing the units described. Do not alter the cost submission sheet; if alterations appear it could be cause for disqualification of the individual submission. Offeror's may add lines as needed on a separate page, maintaining the format given. All fields must have an entry; enter N/A or 0 if the cost does not apply. Line 1-5 represents fixed costs for the initial 48-month term. Line 8 represents a recurring charge for expanded bandwidth, if necessary, while operating out of colocation facility following a disaster at Treasury's main data center. Line 9 represents an annual percentage increase after the initial 48-month fixed term for option years 5-8.

Line	Services	Qty	Recurring/non-recurring	Fee
1	Dedicated Colocation Full Cabinet (48U)	2	Recurring (Monthly)	$
2	208V 30 Amp Power Circuit – 24 Amps or 4.9 kW of useable power via dual feed PDU. The receptacle for power circuit is L6-30R.	2	Recurring (Monthly)	$
3	208 Volt 30 Amp Metered Power Distribution Unit (PDU)	4	Recurring (Monthly)	$
4	Telecom Services Stand Alone Cross-Connect - Cable Type: Single-Mode Fiber (WAN MPLS cross-connect)	1	Recurring (Monthly)	$
5	1 Mbps of internet bandwidth burstable to 1 Gbps	10	Recurring (Monthly)	$
	Total recurring charges			
6	One-time setup (New customer)	-	Non-Recurring	$
7	Incident occurrence	-	Non-Recurring	$
8	Expanded bandwidth for continuous operation at 300 Mbps	-	Recurring (Monthly)	$
9	Escalation percentage associated with optional renewals (Years 5-8)	-	Annual	%

(The service provider agrees that this cost proposal will remain valid for no less than 150 days from the date of proposal submittal.)

Appendix F: Protest Procedures

Protest Procedures For Request for Proposals (RFP)

I. Who May File the Protest. An offeror or prospective offeror or prospective contractor who is aggrieved in connection with the request for proposals (RFP) or award of the contract may file a protest. No protest may be filed if the request for proposals (RFP) is cancelled or if all proposals received in response to the RFP are rejected.

II. Place for Filing. A protest must be filed with the Issuing Office identified in the RFP.

III. Time for Filing.

A. A prospective offeror who is considering filing a proposal must file the protest within seven (7) days after the prospective offeror knew or should have known of the facts giving rise to the protest, but in no event later than the proposal submission deadline specified in the RFP.

B. A protest filed by an offeror who submits a proposal must be filed within seven (7) days after the protesting offeror knew or should have known of the facts giving rise to the protest, but in no event may an offeror file a protest later than seven (7) days after the date the notice of award of the contract is posted on the Treasury Departments website.

C. The date of filing is the date of receipt of the protest.

D. Commonwealth agencies are required by law to disregard any protest received beyond the deadlines established in this Section III.

IV. Contents of Protest.

A. A protest must be in writing.

B. A protest shall state all grounds upon which the protesting party asserts the RFP or contractor selection was improper.

C. The protesting party may submit with the protest any documents or information it deems relevant.

V. Notice of Protest.

A. The Issuing Office will notify the successful offeror of the protest if contractor selection has already been made.

B. If the Issuing Office receives the protest before selection, and it determines that substantial issues are raised by the protest, the Issuing Office will notify all offerors who appear to have a substantial and reasonable prospect of selection.

C. Any offeror notified of a protest pursuant to this Section V. may file its agreement/disagreement with the Issuing Office within the time period specified in the acknowledgement of protest letter sent by the Issuing Office.

VI. Stay of Procurement.

A. The agency head or designee will promptly decide upon receipt of a timely protest whether or not the award of a contract shall be delayed, or if the protest is timely received after the award, whether the performance of the contract should be suspended.

B. The Issuing Office shall not proceed further with the RFP unless the agency head or designee, in consultation with the using agency where applicable, makes a written determination that the protest is clearly without merit or that award of the contract without delay is necessary to

protect the substantial interests of the Commonwealth.

VII. Response and Reply.

A. Within 15 days of receipt of the protest, the Issuing Officer may submit to the agency head or designee and to the protesting party a response to the protest.

B. The protesting party may file a reply to the Issuing Officer's response within ten days of the date of the response.

VIII. Procedures.

A. The agency head or designee shall review the protest and any response or reply.

B. The agency head or designee may decide the merits of the protest on the written, submitted documentation; request and review any additional documents or information deemed necessary to render a determination; or, in his sole discretion, conduct a hearing.

IX. Determination. The agency head or designee shall promptly, but in no event later than 60 days from the filing of the protest unless both parties agree to an extension, issue a written determination. The determination shall:

A. State the reason for the decision, and

B. If the determination is a denial of the protest, inform the protesting contractor of its right to file an action in the Commonwealth Court within fifteen (15) days of the determination mailing date.

The agency head or designee shall send a copy of the determination to the protesting party and any other person determined by the agency head or designee to be affected by the determination.

Appendix G: Data Center Tier Summary

Details	Tier I [1]	Tier II [2]	Tier III [3]	Tier IV [4]
Uptime Requirement	**99.671%**	**99.741%**	**99.982%**	**99.995%**
Downtime Allowance	**29 hours per year**	**22 hours per year**	**1.6 hours per year**	**26.3 minutes per year**
Active components supporting the IT Load	Normal	Normal+1	Normal+1	Normal After any failure
Generator System	Primary Power Source vs Utility	Primary Power Source vs Utility	Primary Power Source vs Utility	Primary Power Source vs Utility
Electrical Distribution Paths	1	1	1 Active 1 Alternate	2 Active at same time
Cooling Distribution Paths	1	1	1 Active 1 Alternate	2 Active at same time
IT Equipment Power Paths	1	1	1 Active 1 Alternate	2 Active at same time
Concurrently Maintainable	No	No	Yes	Yes
Fault Tolerant	No	No	No	Yes
Compartmentalization	No	No	No	Yes
Dedicated IT Area	Yes	Yes	Yes	Yes
Dedicated Cooling Equipment	Yes	Yes	Yes	Yes
Sufficient IT capacity when a critical component is removed from service	No	Yes	Yes	Yes
UPS Systems	Normal	Normal+1	Normal+1	Normal After any failure
Make-up Water	Normal [12 hours storage]	Normal [12 hours storage]	Normal+1 [12 hours storage]	Normal After any failure [12 hours storage]
Engine Generator Rating	Prime	Prime	Continuous	Continuous
Engine Generator/Fuel Cell	Normal [12 hours storage]	Normal [12 hours storage]	Normal+1 [12 hours storage]	Normal After any failure [12 hours storage]