|  |  |
| --- | --- |
| Appendix a: Written Response Packet | |
| Solicitation Number: | RFQ 24-01 |
| Title: | Cybersecurity Services |
| Issuer: | Florida Prepaid College Board  1801 Hermitage Boulevard, Suite 210  Tallahassee, FL 32308 |
| When completing this Written Response Packet, the Respondent should give clear, concise, and, where appropriate, quantifiable replies to all questions. The length of the Response is at the discretion of the Respondent; however, Responses are expected to be brief and to contain full and fair disclosure of essential elements without references to an appendix or attachment, unless otherwise requested. Respondents shall only propose one product against one benchmark.  This packet is made available in Microsoft Word on the Board’s website for ease of completion.  Please visit: [myfloridaprepaid.com/who-we-are/about-the-board/board-reports-and-plans/](http://www.myfloridaprepaid.com/who-we-are/about-the-board/board-reports-and-plans/). | |

|  |  |
| --- | --- |
| TAB 1: REQUEST FOR QUOTE ACKNOWLEDGEMENT | |
| Solicitation Number: | RFQ 24-01 |
| Title: | Cybersecurity Services |
| Issuer: | Florida Prepaid College Board  1801 Hermitage Boulevard, Suite 210  Tallahassee, FL 32308 |
| This sheet and the accompanying negotiation documents constitute an offer from the Respondent to provide the services detailed in the solicitation under the contractual terms provided therein.  By completing this acknowledgment, I agree to abide by all conditions of this negotiation and certify that (1) I am authorized to sign this response and (2) that the offer complies with all requirements of the solicitation. | |
| Respondent (Firm): |  |
| Contact Person: |  |
| Address: |  |
|  |  |
| Telephone: |  |
| E-Mail Address: |  |
| Authorized Signature: |  |
| Date: |  |
| Printed Name & Title: |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tab 2: Minimum and preferred Qualifications | | | | |
| Solicitation Number: | RFQ 24-01 | | | |
| Title: | Cybersecurity Services | | | |
| Respondent: |  | | | |
| The following represent minimum qualifications. A mark in a field indicates an affirmative response to the statement. Any Respondent that does not satisfy the criteria herein shall be rejected. | | | | |
| Minimum Qualifications | |  |  | Yes/No |
| The Respondent has a minimum of five years’ experience providing cybersecurity advisory services to either federal, state, or local governments or financial services related customers. | |  |  |  |
| The Respondent has their principal place of business and corporate charter located and registered in the United States. | |  |  |  |
| The Respondent agrees to provide the services and agrees to all other requirements as stated in the RFQ. | |  |  |  |
| The Respondent will agree to propose project resources that are U.S. based. | |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Preferred Qualifications |  |  | Yes/No |
| The Respondent has experience providing cybersecurity advisory services to financial services organizations that provide transactional payment, investment, and savings account management, 529 programs and educational institution payment services. |  |  |  |
| The Respondent has experience providing cybersecurity advisory services related to use of Salesforce platform including Financial Services Cloud, Experience Cloud, Marketing Cloud, MuleSoft and other Salesforce products as enterprise transactional systems. |  |  |  |
| The Respondent has experience providing cybersecurity services to State or Federal public sector clients. |  |  |  |

|  |  |
| --- | --- |
| Tab 3: Organizational Experience | |
| Solicitation Number: | RFQ 24 – 01 |
| Title: | Cybersecurity Services |
| Respondent: |  |
|  | |
| **Organization Overview** | |
|  | |
| 1. Introduce the Respondent by providing a brief overview of:    1. History    2. Services provided    3. Location(s)    4. Ownership structure    5. Number of employees  |  | | --- | |  | | |
|  | |
| 1. Provide background information about your company, including how many years in business, number and industries of clients served, annual revenue, and any awards or certifications received, including PII, PCI, SOC1 and/or SOC2 certifications.  |  | | --- | |  |  1. Provide the name, contact information and a brief description of services provided for at least three relevant clients. The Board may contact these individuals during due diligence efforts. | |
|  | |
|  | |
| 1. Describe your organization’s experience, if any, with similar organizations or industries to the Board. Provide example of specific cybersecurity challenges that you have successfully addressed in previous engagements.  |  | | --- | |  |  1. Describe how your organization approaches selecting and implementing security technologies for an organization.  |  | | --- | |  |  1. Describe how your organization manages regular communication and updates to executive leadership.  |  | | --- | |  | | |
|  | |
| **Regulatory Restrictions, Litigation and Conflicts of Interest** | |
|  | |
| 1. State whether or not there are any past or pending regulatory restrictions, consent orders, stipulations or litigation to which the Respondent, any subcontractor, any Related Entity of the Respondent or any subcontractor, or any of their principals, owners, directors or officers, has ever been a party that would affect its or their ability to provide the required services or which alleges any unfair, illegal or unethical business practice. If so, a detailed description of each must be provided. | |
|  | |
|  | |
| 1. State whether or not any penalties, fines or liquidated damages have been imposed against the Respondent, any subcontractors or any Related Entity of the Respondent or any subcontractor, including without limitation thereto, those associated with any contract for services entered into by the Respondent, any subcontractor, or any Related Entity of the Respondent or any subcontractor, within the past five (5) years. If so, a detailed description of each such incident, including the amount of the penalty, fine, or liquidated damages imposed, must be included in the Response. | |
|  | |
|  | |
| 1. State whether or not the Respondent or any subcontractor has ever been involved in any litigation with any Qualified Tuition Plan. If so, a detailed description of each lawsuit must be provided. | |
|  | |
|  | |
| 1. State whether or not the Respondent or any Related Entity has ever been contacted by any regulatory body (federal, state or industry) regarding any potentially illegal, non-compliant, unethical or improper activities involving the Respondent, any Related Entity, or any of the employees of the Respondent or any Related Entity. If so, a detailed description must be provided that indicates whether your firm or any Related Entity conducted an investigation of those matters. | |
|  | |
|  | |
| 1. Confirm that the Respondent has not been placed on the convicted vendor list and that it will comply with the provisions of s. 287.133, F.S. Section 287.133(2)(a), F.S., which provides:   *A person or affiliate who has been placed on the convicted vendor list following a conviction for a public entity crime may not submit a bid, proposal, or reply on a contract to provide any goods or services to a public entity; may not submit a bid, proposal, or reply on a contract with a public entity for the construction or repair of a public building or public work; may not submit bids, proposals, or replies on leases of real property to a public entity; may not be awarded or perform work as a contractor, supplier, subcontractor, or consultant under a contract with any public entity; and may not transact business with any public entity in excess of the threshold amount provided in s. 287.017 for CATEGORY TWO for a period of 36 months following the date of being placed on the convicted vendor list.* | |
|  | |
|  | |
| 1. Confirm that the Respondent has not been placed on the discriminatory vendor list and that it will comply with the provisions of s. 287.134(2)(a), F.S. which provides that:   *An entity or affiliate who has been placed on the discriminatory vendor list may not submit a bid, proposal, or reply on a contract to provide any goods or services to a public entity; may not submit a bid, proposal, or reply on a contract with a public entity for the construction or repair of a public building or public work; may not submit bids, proposals, or replies on leases of real property to a public entity; may not be awarded or perform work as a contractor, supplier, subcontractor, or consultant under a contract with any public entity; and may not transact business with any public entity.* | |
|  | |
|  | |
| 1. Pursuant to the provisions of Chapter 112, F.S., Respondents must disclose with their Response the name of any officer, director, or agent who is also an employee of the State of Florida, the Board, or any State agency. Respondents must disclose the name of any state employee who owns, directly or indirectly, interest of five percent or more in the Respondent. Respondents must disclose all investment products, annuities, mutual funds or other similar type savings plans that are marketed or sold by the Respondent or its proposed subcontractors for other states as a part of a prepaid college fund or a college savings fund. | |
|  | |

|  |  |
| --- | --- |
| Tab 4: Cybersecurity services | |
| Solicitation Number: | RFQ 24-01 |
| Title: | Cybersecurity Services |
| Respondent: |  |
| 1. Describe how your organization approaches cybersecurity risk assessments, specifically when assessing third-party vendors, and what methodologies are used? Provide any example of a successful vendor risk management strategy that your organization has implemented.  |  | | --- | |  |  1. Provide examples of risk mitigation strategies that your organization has implemented for similar clients.  |  | | --- | |  | | |
| 1. Describe how your organization ensures that cybersecurity measures are continually improving for your clients? Provide an example of continuous improvement initiative that your organization has implemented.  |  | | --- | |  |  1. Describe how your organization will align cybersecurity strategies with the Board’s business objectives. Provide examples of the Board’s industry's specific cybersecurity challenges.  |  | | --- | |  |  1. Describe how your organization will communicate cybersecurity matters to non-technical stakeholders, including executives and board members? Provide any relevant examples of a successful communication strategy.  |  | | --- | |  |  1. Describe your organization’s expertise and experience in ensuring compliance with relevant cybersecurity regulations and standards. Provide any relevant experience related to assisting clients navigating compliance audits.  |  | | --- | |  |  1. How will your organization assist in development and implementation of an effective security awareness training program for the Board employees, members, and third-party vendors? Provide an example of how you have improved security awareness through the successful implementation of a training strategy.  |  | | --- | |  |  1. Describe how your organization will go about building or improving a cybersecurity program? Share a scenario where you enhanced a security program through incremental improvements.  |  | | --- | |  |  1. Describe your organization’s approach in assisting organizations in the development, testing, and continuous improvement of incident response and business continuity and disaster recovery.  |  | | --- | |  | | |
|  | |

|  |  |  |
| --- | --- | --- |
| Tab 5: VALUE-ADDED SERVICES | |  |
| Solicitation Number: | RFQ 24-01 |  |
| Title: | Cybersecurity Services |  |
| Respondent: |  |  |
|  | |  |

|  |
| --- |
| **Value-Added Services** |
| |  | | --- | | For eachValue-Added Service, describe the service your organization offers that may provide enhanced benefits to the Board, including operational efficiencies, cost savings, etc. The description should include:   1. Overview of the service 2. Benefits to the Board of receiving or utilizing the service 3. One-time and ongoing cost to the Board for receiving or utilizing the service 4. Expectations or requirements of the Board in order to begin receiving or utilizing the service 5. Implementation activities necessary to be performed to begin receiving or utilizing the service | |  | |

|  |  |  |
| --- | --- | --- |
| Tab 6: Pricing Schedule | |  |
| Solicitation Number: | RFQ 24-01 |  |
| Title: | Cybersecurity Services |  |
| Respondent: |  |  |
| The Board is open to the Respondent’s recommended pricing model based on the services requested. Please use the below chart to specify your pricing model, including the breakdown of fixed cost and project-based costs and Value-Added Services. | |  |

|  |  |
| --- | --- |
|  |  |
| **Fixed Price** | | | | |
| **Description of Service** | | | **Frequency** | **Item Total** |
|  | | | Monthly |  |
|  | | | Monthly |  |
|  | | | Monthly |  |
|  | | | Monthly |  |
| **Total** | | |  |  |

|  |  |
| --- | --- |
| **Variable Project Costs** | |
| **Description of Services** | **Price** |
|  |  |
|  |  |
|  |  |
|  |  |

|  |
| --- |
|  |