**Exhibit A**



**State of Vermont Bidder Response Form**

**Request for Proposal Name: OCS OmniChannel Payment Platform**

**Vendor Instructions:**

Provide the information requested in this form and submit it to the State of Vermont as part of your Request for Proposal (RFP) response. All answers must be provided within the form unless otherwise specified.

**Important: This form must be completed and submitted in response to this RFP for your proposal to be considered valid. The submission must also include the eight (8) additional artifacts requested within this form (denoted by underlined green font).**

## See the RFP for full instructions for submitting a bid. **Bids must be received by the due date and at the location specified on the cover page of the RFP.**

Direct any questions you have concerning this form or the RFP to:

**STATE CONTACT: Roland Ortiz**

**TELEPHONE: (802) 371-8987**

**EMAIL:** **sov.ThePathForward@vermont.gov**

## **Part 1: VENDOR PROFILE**

1. Complete the table below.

|  |  |
| --- | --- |
| **Item** | **Detail** |
| Company Name:  | [insert the name that you do business under] |
| Physical Address: | [if more than one office – put the address of your head office] |
| Postal Address: | [e.g. P.O Box address] |
| Business Website: | [URL address] |
| Type of Entity (Legal Status): | [sole trader/partnership/limited liability company or specify other]  |
| Primary Contact: | [name of the person responsible for communicating with the Buyer] |
| Title: | [job title or position] |
| Email Address: | [email] |
| Phone Number: | [landline] |
| Fax Number: | [fax] |

1. Provide a brief overview of your company including number of years in business, number of employees, nature of business, and description of clients. Identify any parent corporation and/or subsidiaries.

1. Is your organization currently or has it previously provided solutions and/or services to any agency or entity of the Vermont State government? If so, name the State entity, the solution and/or services provided, and the dates.
2. **Provide a Financial Statement\* for your company and** **label** **it Attachment #1**. A confidentiality statement may be included if this financial information is considered non-public information. This requirement can be filled by:
	* A current Dun and Bradstreet Report that includes a financial analysis of the firm;
	* An Annual Report if it contains (at a minimum) a Compiled Income Statement and Balance Sheet verified by a Certified Public Accounting firm; or
	* Tax returns and financial statements including income statements and balance sheets for the most recent 3 years, and any available credit reports.

*\*Some types of procurements may require bidders to provide additional or specific financial information. Any such additional requirements will be clearly identified and explained within the* *RFP, and may include supplemental forms in addition to this Bidder Response Form.*

1. Disclose any judgments, pending or expected litigation, or other real potential financial reversals, which might materially affect the viability or stability of your company or indicate below that no such condition is known to exist.

1. Provide a list of three references similar in size and industry (preferably another governmental entity). References shall be clients who have implemented your Solution within the past 48 months.

|  |  |
| --- | --- |
| **Reference 1** | **Detail** |
| Reference Company Name:  | [insert the name that you do business under] |
| Company Address: | [address] |
| Type of Industry: | [industry type: e.g., government, telecommunications, etc.] |
| Contact Name: | [if applicable] |
| Contact Phone Number: | [phone] |
| Contact Email Address: | [email] |
| Description of system(s) implemented: | [description] |
| Date of Implementation: | [date] |
| **Reference 2** | **Detail** |
| Reference Company Name:  | [insert the name that you do business under] |
| Company Address: | [address] |
| Type of Industry: | [industry type: e.g., government, telecommunications, etc.] |
| Contact Name: | [if applicable] |
| Contact Phone Number: | [phone] |
| Contact Email Address: | [email] |
| Description of system(s) implemented: | [description] |
| Date of Implementation: | [date] |

|  |  |
| --- | --- |
| **Reference 3** | **Detail** |
| Reference Company Name:  | [insert the name that you do business under] |
| Company Address: | [address] |
| Type of Industry: | [industry type: e.g., government, telecommunications, etc.] |
| Contact Name: | [if applicable] |
| Contact Phone Number: | [phone] |
| Contact Email Address: | [email] |
| Description of system(s) implemented: | [description] |
| Date of Implementation: | [date] |

## **Part 2: Vendor Proposal/Solution**

1. Provide a description of the technology solution you are proposing.
2. Provide a description of the capabilities of the technological solution you are proposing.
3. If a proprietary software is being proposed, provide a description of the:
	1. Standard features and functions of the software:
	2. The software licensing requirements for the solution:
	3. The standard performance levels:
		* Hours of system availability:
		* System response time:
		* Maximum number of concurrent users:
		* Other relevant performance level information:
4. Give a brief description of the evolution of the system/software solution you are proposing. Include the date of the first installed site and major developments which have occurred (e.g. new versions, new modules, specific features).
5. List the total number of installations in the last 3 years by the year of installation.
6. Provide the total number of current users for the proposed system and indicate what version they are using.
7. Have you implemented the proposed solution for other government entities? If so, tell us who, when, and how that implementation went?
8. Provide a Road Map that outlines the company’s short term and long term goals for the proposed solution/software and label it Attachment #2.
9. **Provide a PowerPoint (minimum of 1 slide and maximum of 10 slides) that provides an Executive level summary of your proposal to the State. Label** **it Attachment #3.**
10. Does your proposed solution include any warranties? If so, describe them and provide the warranty periods.
11. Describe any infrastructure, equipment, network or hardware *required* to implement and/or run the solution.
12. What is your recommended way to host this solution?
13. Describe how your solution can be integrated to other applications and if you offer a standard-based interface to enable integrations.
14. Please describe any options that your solution supports for providing merchant services (i.e. the processing of credit or debit card transactions). For example, does your solution support the ability to integrate with the State’s current merchant services provider, and if so, what implications would that have on your pricing.
15. Respond to the following questions about the solution being proposed:

|  |
| --- |
| **Vendor Response/Explanation** |
| **Question** | **Yes or No** |  |
| 1. Does the solution use Service Oriented Architecture for integration?
 |  |  |
| 1. Does the solution use a Rules Engine for business rules?
 |  |  |
| 1. Does the solution use any Master Data Management?
 |  |  |
| 1. Does the solution use any Enterprise Content Management software?
 |  |  |
| 1. Does the solution use any Case Management software?
 |  |  |
| 1. Does the solution use any Business Intelligence software?
 |  |  |
| 1. Does the solution use any Database software?
 |  |  |
| 1. Does the solution use any Business Process Management software?
 |  |  |
| 1. Is this a browser-based solution and if so, what browsers do you support?
 |  |  |
| 1. Does the solution include an API for integration?
 |  |  |

## **Part 3: Functional Requirements**

The table below lists the State’s Functional Requirements. Indicate the “Availability” for each requirement for your proposed solution. Use the “Vendor Comments” column to provide any additional information or explanations.

**A** - Feature is available in the core (“out-of-the-box”) solution.

**D** - Feature is currently under development (indicate anticipated date of availability in the Vendor comments column).

**C** - Feature is not available in the core solution but can be provided with customization.

**N** - Feature is not available.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID #** | **Functional Requirement Description** | **Availability** | **Vendor Comments** |
| **1 Operational**  |
| A | The Solution must be accessible 24-7 |  |  |
| B | The Solution must display the up-to-date balances owed for the current monthly obligations and arrears (past due amounts) as provided by OCS each day to the payor. For example: NCP may have multiple cases for which they are paying, or Employers make payments for their employees where some of which may have multiple cases |  |  |
| C | The Solution must display prorated obligation amounts for Employers based on their payroll frequency and total monthly obligation as provided by OCS each day |  |  |
| D | The Solution must provide real time validations/ verifications for ACH/eCheck payments |  |  |
| E | The Solution must provide real time validations/ verifications for Debit Card payments |  |  |
| F | Solution must provide role-based access where at a minimum one of the roles is a State Admin role that has elevated permissions such as ability to research payment transactions and access solution reports.  |  |  |
| G | The Solution must include a way to suspend/block specific payment methods for those with repeated failed payments (e.g., after having 3 ACH payments returned for insufficient funds, ACH payments are no longer an option for that payor) |  |  |
| H | The Solution must be able to interface with the State’s preferred financial institution (Bank 1/Lockbox) to securely transmit a payment data text file daily. Please refer to RFP, Table 2.2.1.4 for details. |  |  |
| I | The Solution must be able to interface with the State’s preferred financial institution (Bank 2) to securely deposit those funds processed through the e-Payment Portal. Please refer to RFP, Table 2.2.1.4 for details. |  |  |
| J | The Solution must be able to securely interface with OCS’s Case Management System to receive case-specific data files with case information daily. Please refer to RFP, Item 2.7 for details. |  |  |
| **2 User Experience** |
| A | The Solution must provide multiple payment channels to our OCS paying customers (e.g., web, mobile device, mobile app, kiosk, etc). |  |  |
| B | The Solution must provide multiple payment options for OCS customers to pay child support (e.g., credit card, debit card, PayPal, Venmo, e-check/ACH, etc.) |  |  |
| C | The Solution must provide a web-based user portal that employs current web technologies. |  |  |
| D | The Solution must have verbiage and instructions featured with understanding set at a 7th grade reading level. |  |  |
| E | The Solution must accept and allow payments from multiple types of Payors (e.g., Employers, NCP's, Agents paying on behalf of NCP) |  |  |
| F | The Solution must provide self-service payment options such as Pay-by-Phone. |  |  |
| G | The Solution must employ Interactive Voice Response (IVR). |  |  |
| H | OCS staff must be able to transfer Customers calling and wishing to pay by phone to the IVR service that is PCI compliant. |  |  |
| I | The Solution must provide one-time (immediate and/or future dated) payment options |  |  |
| J | The Solution must provide options to schedule recurring payments |  |  |
| K | The Solution must provide Payors with a capability to securely send notifications, reminders and other communications within the context of the Solution system. |  |  |
| L | Training on the Solution must be provided to limited OCS staff; training can be virtual or onsite; training should occur before “go live” date and whenever there is a major update/release. |  |  |
| M | Training on the Solution payment research and reporting capabilities must be provided to limited OCS staff; training can be virtual or onsite; training should occur before “go live” date and whenever there is a major update/release. |  |  |
| **3 Financial**  |
| A | The Solution must provide Payors with multiple self-service payment channels available through: web |  |  |
| B | The Solution must provide Payors with multiple self-service payment channels available through: mobile device, mobile app |  |  |
| C | The Solution must provide Payors with multiple self-service payment channels available through: Call Center |  |  |
| D | The Solution must provide Payors with multiple self-service payment channels available through: Kiosks |  |  |
| E | The Solution must provide Payors with multiple legacy payment methods: Credit Card |  |  |
| F | The Solution must provide Payors with multiple legacy payment methods: Debit Card |  |  |
| G | The Solution must provide Payors with multiple legacy payment methods: ACH/e-check |  |  |
| H | The Solution must provide Payors with multiple emerging payment methods as well: PayPal, PayPal Credit |  |  |
| I | The Solution must provide Payors with multiple emerging payment methods as well: Venmo |  |  |
| J | The Solution must provide Payors with multiple emerging payment methods as well: Apple Pay |  |  |
| K | The Solution must provide Payors with multiple emerging payment methods as well: Google Pay |  |  |
| L | The Solution must provide Payors with multiple emerging payment methods as well: Amazon Pay |  |  |
| M | The Solution must charge/collect convenience fees at the time a payment is initiated |  |  |

## **Part 4: Non- Functional Requirements**

The tables below list the State’s Non-Functional Requirements. Indicate if your proposed solution complies in the “Comply” column.

**Yes** = the solution complies with the stated requirement.

**No** = the solution does not comply with the stated requirement.

**N/A** = Not applicable to this offering.

Describe how the requirement is met in the “Vendor Description of Compliance” column.

**4.1 Hosting**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID #** | **Non-Functional Requirement Description** | **Comply** | **Vendor’s Description of Compliance**  |
| H1 | Any technical solution must be hosted in a data center. |  |  |
| H2 | Any hosting provider must document and implement back-up and disaster recovery plans to be approved by the State.  |  |  |
| H3 | Any hosting provider will implement best practices for change requests, incident management, problem management and service desk services in accordance with the Information Technology Infrastructure Library (ITIL).  |  |  |

**4.2 Application Solution**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID #** | **Non-Functional Requirement Description** | **Comply** | **Vendor’s Description of Compliance**  |
| A1 | Any solutions vendor must provide for the data backup data recovery, data retention policies and disaster recovery procedures for the Solution system to be approved by the State.  |  |  |
| A2 | Any solutions vendor must engage the State of Vermont using Service Level Agreements for system and application performance, incident reporting and maintenance.  |  |  |
| A3 | The State owns any data they enter, migrate, or transmit into the solution and the vendor shall allow the State to pull or copy this data at any time free of charge.  |  |  |
| A4 | The solution must provide clear and accurate documentation and guidance for the customers and users on how to use the service effectively and efficiently. |  |  |
| A5 | The software shall document any changes made to the software between versions, so that users understand potential issues when upgrading. This documentation should be easily accessible and understandable for non-technical users. |  |  |
| A6 | The solution must have clear and detailed documentation, including design and architecture documents, API specifications, and user manuals. |  |  |
| A7 | Solutions Providers will provide version control management capability. All changes to Solutions will be reported and approved by the State and will be maintained in the Solutions Provider's version control management solution, which will be available to the State for review and audit. |  |  |
| A8 | The system will provide auditing and internal capabilities to generate audit logs. |  |  |
| A9 | The solution must support automated analysis tools for identifying and reporting on issues such as code quality, security vulnerabilities, and performance bottlenecks. |  |  |
| A10 | To maintain the accuracy and integrity of the data, SaaS and PaaS solution providers must perform regular data system refreshes. |  |  |
| A11 | Proposed solutions for managing business processing rules will include functionalities such as rule extensibility, mapping rules to owners and stewards, impact analysis of rule changes, integration and coordination of distributed rule engines with a corporate master, rerunning the engine for a previous point in time, entering future rule changes, performing consistency and collision checks, supporting rule versioning and release versioning with rollback features, ensuring rule security, and associating rules with multiple program profiles. |  |  |
| A12 | As part of the Run Book delivered prior to go-live, the Solutions Provider must maintain a logical Architecture Document that outlines the current configuration of all modular components, including third-party applications, in all environments. |  |  |
| A13 | 3rd party software applications that are cloud and SaaS products are natively integrated with no special integration required to connect or sync data. |  |  |
| A14 | If required for the solution, Solutions Providers will submit to the State as part of their proposal: Specifications for all necessary hardware, software, and tools for up to six (6) target environments: 1. Production (PRD), 2. Staging (STG), 3. Development (DEV), 4. Test (TST), 5. Training (TRN), and 6. Disaster Recovery (DR). |  |  |
| A15 | When proposing changes to the architecture of the solution, the solution provider will generate an updated logical architecture diagram. |  |  |
| A16 | Solutions will have documentation for assisting rule authors and administrators with best practices for rule repository creation and maintenance, repository check-in/checkout, and repository promotion across environments. Solutions will include text documentation and meta-data in the rule's repository. |  |  |
| A17 | Solutions Providers will provide the required system permissions, documentation and training that describes the procedures for Solution administrators to add, update or inactivate user IDs and passwords. |  |  |
| A18 | Solutions Providers will deliver to the State a Requirements Traceability Matrix (RTM) for all delivered functionality, showing all tested activities traced to delivered functionality, and all delivered functionality traced to requirements in the requirements repository. |  |  |
| A19 | Self-paced online training modules for the following user roles shall be available at no additional cost. |  |  |
| A20 | Before any release or changes are made, Solutions Providers will collaborate with the State and other Solutions Providers as needed, to test the functionality and usability of the release (User Acceptance Testing or UAT), confirm that the release meets the business requirements and needs, and train to ensure the smooth operation of the State's applications and solutions. Solutions Providers will also document any application changes and create training materials for end users, covering defect resolution, workarounds, updates and changes requested by the State. |  |  |
| A21 | The solution provider will provide an Availability Plan for the SaaS and PaaS solution. The Availability Plan must include the following: Availability Objectives base on the SLA Availability Architecture - high availability, DR, and data protection Availability Management - Roles and Responsibilities, RACI, specific processes, and procedures for reporting, analyzing and resolving incidents, and communication with stakeholders.  |  |  |
| A22 | The solution provider will obtain advance approval from the State for changes to infrastructure components that will be implemented outside the standard Maintenance Windows and will affect functionality.  |  |  |
| A23 | The solution provider will comply with Service Level Agreements for the solution.  |  |  |
| A24 | Solutions will provide the ability to recover from data loss due to end user error and end application error. Recovery includes the following: a. The solutions will be able to restore or recover any data that is lost due to various reasons, such as hardware failure, network outage, human error, or malicious attack. b. Due to end user error: The solutions will be able to recover from data loss caused by mistakes or errors made by the end users of the solutions, such as deleting or modifying data accidentally or incorrectly. c. Due to end application error: The solutions will be able to recover from data loss caused by errors or bugs in the end applications that use the solutions, such as crashing, freezing, or corrupting data.  |  |  |
| A25 | The solution provider will inform the State when it plans to use something other than those designated for routine maintenance and State-specific Release Management tasks. |  |  |
| A26 | The solution provider will validate that each interface is working correctly. The solution provider will resolve all interface-related problems caused by solution provider-developed interfaces.  |  |  |
| A27 | The solution provider will report Outages and Service Interruptions when identified per the SLA.  |  |  |
| A28 | The solutions provider will send alarms based on the monitored attributes. These will be escalated through eMail and SMS.  |  |  |
| A29 | The solution provider will schedule routine planned maintenance activities without disrupting the operational hours.  |  |  |
| A30 | The solution provider will assist the State in identifying root causes for all Solution interface related problems. |  |  |
| A31 | The PaaS and SaaS solutions provider will supply environments that are scalable, enterprise-ready applications. These include sandboxes, testing platforms, staging platforms and development platforms as needed for the solution.  |  |  |
| A32 | The solution provider will apply changes at the component and data level with no loss of availability at the application or component level (modular component modifiability).  |  |  |
| A33 | As part of Monitoring Services, the solution provider will use information collected by tools to monitor use, performance, and availability of the solution provider Programs and to resolve service requests.  |  |  |
| A34 | The solution provider will perform problem analysis and make recommendations to the State of activities that may enhance service quality and reduce recurrence of Incidents affecting availability. These include the following: a. Perform problem analysis: The solution provider will investigate and identify the root causes of any incidents that affect the availability of the solution. b. Make recommendations to the State: The solution provider will suggest actions or improvements to the State that can help prevent or reduce the recurrence of incidents affecting availability. c. Enhance service quality: The solution provider will aim to improve the value and satisfaction delivered by the solution to the State and its users. d. Reduce recurrence of incidents affecting availability: The solution provider will try to minimize the number and frequency of incidents that disrupt access to or use of the solution.  |  |  |
| A35 | The solution provider will provide the status of Root Cause Analysis for Severity Level 1 Unplanned Outages, as defined in Service Level Agreement.  |  |  |
| A36 | The solution provider will conduct an implementation readiness review at least ten days prior to production cutover.  |  |  |
| A37 | The solution provider will be accountable for all end-to-end and integration testing for the applications that they built including all external interfaces.  |  |  |
| A38 | In advance of any release or changes the solution provider will produce for the State the following: a. Change release documentation: that describes the changes made to the solution such as new features, bug fixes, and enhancements. b. Updated test scripts: instructions or commands that are used to verify the functionality and quality of the solution or system after changes have been made. c. Training: instructions on how to use the update to the solution; will allow the State team to adequately test, verify, and train for support of smooth operation of the State's applications and solutions.  |  |  |
| A39 | The solution provider will prepare User Acceptance Testing (UAT) Plan to include, Unit, Integration, SIT, Regression, Stress/Performance.  |  |  |
| A40 | The solution provider is responsible for restoring the normal operation of the Production Environment, which is where the users can access and use the hosted services and data.  |  |  |
| A41 | The State of Vermont (SOV) will access applications through a URL entered in a web browser. |  |  |
| A42 | The solution should be designed to provide secure, scalable, and accessible storage and retrieval of policy and procedures documents, allowing users to quickly and easily find and access the information they need. The application should have robust search capabilities, support version control, and enable collaboration among multiple stakeholders. |  |  |
| A43 | The solution should conform to the web accessibility guidelines specified by the W3C level 2 accessibility guidelines, ensuring that the application is accessible to users with disabilities. The system should meet the standards outlined in the guidelines to provide an inclusive and user-friendly experience for all users, regardless of their abilities. The application should be designed to accommodate a wide range of assistive technologies and should be tested to ensure compliance with accessibility guidelines. |  |  |
| A44 | Solutions will adhere to all Federal and Vermont accessibility requirements, or their successors: Section 508 of the Rehabilitation Act, section 1194.22 of the Code of Federal Regulations, web-based intranet and internet information and applications. |  |  |
| A45 | Information will be provided to applicants and enrollees in plain language and in a manner that is accessible and timely. Individuals living with disabilities including accessible web sites and the provision of auxiliary aids and services at no cost to the individual in accordance with the Americans with Disabilities Act and sections 504 / 508 of the Rehabilitation Act. Individuals who are limited English proficient through the provision of language services at no cost to the individual, including oral interpretation, written translations. Taglines in non-English languages indicating the availability of language services. |  |  |
| A46 | Solutions will provide speech and hearing-impaired people with the ability to communicate through a Teletypewriter (TTY) or Telecommunications Display Device (TDD). |  |  |
| A47 | The application should be able to associate effective dates with every program and rule in the rules engine, allowing for efficient tracking and management of changes to the system over time. |  |  |
| A48 | Solutions will roll-up (summarize data) and drill-down (view details) in reports online. |  |  |
| A49 | The system should provide the ability to create, customize and interact with the system and should provide the ability to create, customize and interact with multi-dimensional views and tables, enabling users to explore data and gain insights into complex relationships between various dimensions. |  |  |
| A50 | Solutions will provide the ability to identify all other rules that are dependent on a specific rule by allowing rules association. |  |  |
| A51 | Solutions will provide context sensitive help and extensive documentation. |  |  |
| A52 | Service Providers will develop a user guide that can be accessed online and printed on demand. |  |  |
| A53 | Solutions will permit all users (dependent on role-based security and access rights) to have current and up-to-date information regarding a client's information when connected to solutions, given the operational and technical constraints of the data source(s). The data displayed will be time-stamped to reflect the currency of the data. |  |  |
| A54 | Solutions will support reporting requirements either natively or integrate with other reporting tools to provide reporting. |  |  |
| A55 | Solutions will provide the capability to identify and apply a rule change appropriately to existing cases. |  |  |
| A56 | Solutions must have the capability to assist in making decisions that involve multiple steps or stages. This may involve providing tools or functionality to help with tasks such as gathering and analyzing data, comparing options, and evaluating trade-offs. The solution should also be able to handle complex decision-making processes that involve multiple criteria, factors, and stakeholders. |  |  |
| A57 | Solutions will provide the capability for documents to be grouped together during scanning based on user defined criteria. |  |  |
| A58 | Solutions will provide access to standardized reporting, ad hoc queries, and data visualization. |  |  |
| A59 | Solutions will provide reports to users in online and offline formats, e.g., web, email, SMS, fax, and hard copy paper. |  |  |
| A60 | The solution should support table-driven variables instead of hardcoded values, enabling users with appropriate role-based permissions to add, delete, update, or view values and rows. The system must be able to immediately access these values based on the effective date ranges of the modified or added records. |  |  |
| A61 | Solutions will provide index-based search capabilities. |  |  |
| A62 | Solutions will provide the ability to store electronic forms (solution generated or 3rd-party generated forms). |  |  |
| A63 | Solutions will provide the capability to access the output of the document management system over the Internet and/or Intranet web sites via web services. |  |  |
| A64 | Solutions will provide the capability to permanently delete documents based on user defined criteria. |  |  |
| A65 | Solutions will provide the ability for user to create and customize reports, queries, and dashboards. |  |  |
| A66 | Solutions will notify and distribute reports based on user specified criteria. |  |  |
| A67 | Solutions may schedule the generation of reports at specific times based upon user's option. |  |  |
| A68 | Solutions will generate ad-hoc and standard reports in real time, as well as historical for incoming and outgoing contacts. |  |  |
| A69 | Solutions will allow for user analytics to be captured and reported. |  |  |
| A70 | Solutions will provide time-based content expiration and version management capabilities. |  |  |
| A71 | Solutions will provide support for full text search. |  |  |
| A72 | Solutions will provide the ability to scan, capture and store solution-generated documents and store them at object level, e.g., contact, case, application, or service request. |  |  |
| A73 | The system should be capable of electronically validating data captured from specific fields on forms that are read by OCR (Optical Character Recognition), OMR (Optical Mark Recognition), or ICR (Intelligent Character Recognition) technology. The solution should be able to verify the accuracy and completeness of the captured data by comparing it against predefined criteria, rules, or reference data. This capability will ensure that the system can effectively process and use the captured data in downstream workflows and processes. |  |  |
| A74 | The solution will support dynamic rule change, enabling users to modify rules on the fly without requiring system downtime. The solution should also separate rules from the engine, making it easier to update rules without affecting the underlying engine. |  |  |
| A75 | Solutions will provide notification features for files that are checked out, overdue, and determined availability. |  |  |
| A76 | Solutions will highlight and flag required and incomplete data fields. |  |  |
| A77 | Solutions will provide the capability to notify the user when a duplicate document has been received, so the user can decide whether to use the previously received document, replace the existing document or store the new document separately. |  |  |
| A78 | Solution error messages will be expressed in plain language, precisely indicate the problem, and constructively suggest a solution. |  |  |
| A79 | Solutions will provide the ability to suggest or automatically change entries that do not conform to data entry standards. |  |  |
| A80 | Solutions will allow the users to easily navigate to a variety of functions available to them without having to move sequentially through excessive menus and screens. |  |  |

**4.3 Security**

As a solution vendor, you must have documented and implemented security practices for the following and have a process to audit/monitor for adherence. Indicate “Yes” or “No” in the “Comply” column or “N/A” if the requirement is not applicable to this offering. Use the “Vendor Description of Applicable Security Processes” column to describe how you meet the requirement and the “Audit/Monitor” column to indicate how you monitor for compliance.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID #** | **Non-Functional Requirement Description** | **Comply**  | **Vendor’s Description** **of Applicable Security Processes**  | **Audit/Monitor Process** |
| S1 | Vendor will provide the state with a Risk Assessment Practices document to include, but not limited to, descriptions of vulnerability and penetration testing procedures. |  |  |  |
| S2 | Vendor will provide the State documentation of its incident response planning and testing procedures |  |  |  |
| S3 | Vendor will provide State with a System Security Plan for review and approval. |  |  |  |
| S4 | Data center facilities will be located in the United States. If the solution contains Federal Tax Info (FTI) or other sensitive data, FedRamp is required. |  |  |  |
| S5 | Vendor will deploy SSL for all Web-based applications for Vendor deployments that involve Internet-facing deployments and for deployments that are accessible through a secure network, e.g., hardware VPN. SSL will be used for data transmitted through all Vendor Web-based applications. |  |  |  |
| S6 | The Vendor will procure and renew SSL certificates on State's behalf. |  |  |  |
| S7 | Least Privilege and Separation of Duties (SOD) will be employed for all solutions. It is a system-oriented approach where user permissions and system functionality are carefully evaluated, and access is restricted to the resources required for users or systems to perform their duties based on role-based access (RBA) to data. |  |  |  |
| S8 | Prior to deployment, new deployments in the Vendor Data Centers will undergo a security technical review by a cross-organization team including a dedicated security team. Technology or tools that do not meet Vendor ’s security policies or standards will not be deployed. |  |  |  |
| S9 | Access controls to network, system, database, and application layers will be multi-tiered and accessible on a default-deny basis. |  |  |  |
| S10 | Deployment environments will be configured with the same security and compliance standards whether production or non-production. |  |  |  |
| S11 | Access to operating systems will be controlled by a secure login procedure that requires a unique user ID and a strong password. |  |  |  |
| S12 | Vendor employees will be required to maintain the confidentiality of state data. Employees may be required to sign a confidentiality agreement and comply with company policies concerning protection of confidential information (Code of Ethics and Business Conduct, Vendor Acceptable Use Policy for Company Resources, and the Information Protection Policy) as part of their initial terms of employment. Vendor will obtain a written confidentiality agreement from each subcontractor before that subcontractor provides services. |  |  |  |
| S13 | Vendor will conduct Security reviews, assessments, and audits periodically to confirm compliance with the Vendor Information Security Policy, procedures, and practices. Employees who fail to comply with the Information Security Policy, procedures and guidelines will be subject to disciplinary action including termination. |  |  |  |
| S14 | Vendor will employ network controls to address the protection and control of the State data during its transmission from one end system to another. All computers, Servers, and other data devices connected to the Vendor network will comply with Vendor standards for security, configuration, and access method, in accordance with the Vendor policies. |  |  |  |
| S15 | Vendor will provide database activity logging, monitoring, and reporting of the production database instances and provide audit reports. |  |  |  |
| S16 | Vendor will employ the use of dedicated backup servers |  |  |  |
| S17 | Vendor will employ intrusion detection systems to provide continuous surveillance for intercepting and responding to security events as they are identified. |  |  |  |
| S18 | Vendor will test the Information Security Incident Response Plan (ISIRP) once per year. Chief-Level, e.g., a CEO, a CIO or a CTO executive approval is required for unscheduled testing. |  |  |  |
| S19 | Vendor will periodically test its incident response procedures under the direction of an incident commander. At the conclusion of each test, the commander will submit a gap analysis report to incident response management along with recommendations for corrective actions. |  |  |  |
| S20 | Security assessments will be performed prior to releasing solutions into production. |  |  |  |
| S21 | Vendor will maintain a Vendor Information Security Policy which describes the principles for development, executive approval, implementation, and maintenance of all information security policies and practices at Vendor. Security Includes governing principles, e.g., need to know, Least Privilege, and Separation of Duties. Employees, Service Providers and temporary employees are subject to the Vendor Information Security Policy. |  |  |  |
| S22 | Upon termination of services, Vendor will return information held in paper form to the State or destroy in accordance with the Vendor Information Protection Policy. |  |  |  |
| S23 | Vendor will acknowledge that the State will be subject to audits by entities other than regulators. If the information required for such an audit is not contained in a SSAE 16 or ISAE 3402 report, the Vendor will make reasonable efforts to provide the required information to the auditor. |  |  |  |
| S24 | Vendor will enable database auditing. |  |  |  |
| S25 | Servers will enable default log file settings for auditing critical events |  |  |  |
| S26 | Integrity of the data-in-transit will be protected through the use of strong encryption (TLS/SSL or IPSec) protocols. Vendor will configure a hashed Message Authentication Code - Secure Hash Algorithm (HMAC-SHA-1) on all IPSec VPN networks to verify that the contents of the transmission have not been altered in transit. |  |  |  |
| S27 | Vendor will monitor, alert, and protect against web application attacks of internet-facing applications. Vendor will install, configure, and manage a web application firewall on Vermont’s internet-facing Environments. |  |  |  |
| S28 | Vendor will provide to the State relevant Breach, Security, or Enforcement policies. |  |  |  |
| S29 | Solutions will detect intrusion attempts by unauthorized system users. |  |  |  |
| S30 | Solutions will allow Solution administrators to create and manage user accounts. |  |  |  |
| S31 | Solutions will transmit reports to various designated recipients in a secure manner. |  |  |  |
| S32 | Solution's interfaces will secure and protect the data and the associated infrastructure from a confidentiality, integrity and availability perspective. |  |  |  |
| S33 | Solutions will use authorization and access control for file level security. |  |  |  |
| S34 | Solutions will use role-based access to display content. |  |  |  |
| S35 | Strong authentication will be employed in all deployment environments. |  |  |  |
| S36 | Database data will be encrypted at the file system layer. |  |  |  |
| S37 | Data stored on file systems will be encrypted. |  |  |  |
| S38 | Vendor, Service Providers and all Subcontractors will comply with all Federal, state, and agency regulations as contained in the Source Docs tab of this document. It is the responsibility of each party to stay current with legal changes acting as an agent of the State of Vermont in compliance with the applicable laws and regulations. Any conflicts in compliance with Source Documents regulations will be reported to the State for the State's direction on how to comply. |  |  |  |
| S39 | Service Provider will review and certify that the code and any new development meets or exceeds the OWASP Application Development Security Standards outlined on the www.OWASP.org site (currently https://www.owasp.org/images/4/4e/OWASP\_ASVS\_2009\_Web\_App\_Std\_Release.pdf ) and document in writing that they have been met. |  |  |  |
| S40 | Servers will have operating systems hardened by eliminating unnecessary system services, accounts, network services, limited user access rights throughout the environments. |  |  |  |
| S41 | Contractor employees who handle regulated data are required to complete a data privacy awareness training course. The course instructs employees on the definitions of data privacy and personal data, recognizing risks relating to personal data, understanding their responsibilities for data, and reporting any suspected privacy violations. Employees handling data are also required to complete training in corporate ethics. Additionally, employees involved in development of custom code are required to attend secure coding training. |  |  |  |
| S42 | The Contractor must ensure all systems undergo Industry Standard security testing (e.g., penetration, physical security, web application, social engineering, and vulnerability tests) minimally on an annual basis, as mutually agreed upon between the Contractor and the State when there has been a significant infrastructure change or resulting from Federal requirements. This security testing must be conducted at no cost to the State and by a State‑approved third party that maintains no financial or controlling relationship with The Contractor. Additionally, The Contractor must provide documented testing results and generate corrective action plans for any deficiencies identified as well as be responsible for modifications to remain compliant based on the terms and conditions of the Contract. |  |  |  |
| S43 | The solution must encrypt data at rest, at transfer, and backed‑up data per FIPS 140‑2 Standards. |  |  |  |
| S44 | Deployment environments will be configured with the same security and compliance standards whether production or non-production. |  |  |  |
| S45 | The Solution must integrate with the State’s preferred identity and access management framework.  |  |  |  |

**4.4 Other Non-Functional Requirements** *N/A*

For each requirement listed, indicate if and how you comply or type “N/A” if it is not applicable to your offering.

**4.5 Data Compliance**

Vendors and their solutions must adhere to applicable State and Federal standards, policies, and laws based on the type of data that will be stored, accessed, transmitted and/or controlled by the solution. If the “Type of Data” column is checked below, respond “Yes” or “No” in the “Comply” column and provide an explanation on how you comply in the “Vendor’s Description of Compliance” column.

|  |  |  |  |
| --- | --- | --- | --- |
| **Type of Data** | **Applicable State & Federal** **Standards, Policies, and Laws**  | **Comply** | **Vendor’s Description** **of Compliance** |
| ☒ Publicly available information  | * [NIST 800-171](https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final)
 |  |  |
| ☒ Confidential Personally Identifiable Information (PII)  | * [State law on Notification of Security Breaches](http://legislature.vermont.gov/statutes/section/09/062/02435)
* [State Law on Social Security Number Protection](http://legislature.vermont.gov/statutes/section/09/062/02440)
* [State law on the Protection of Personal Information](https://legislature.vermont.gov/statutes/fullchapter/09/062)
* National Institute of Standards & Technology:  [NIST SP 800-53](https://nvd.nist.gov/800-53) Revision 4 “Moderate” risk controls
* [Privacy Act of 1974, 5 U.S.C. 552a](https://www.justice.gov/opcl/privacy-act-1974).
 |  |  |
| ☒ Payment Card Information   | * [Payment Card Industry Data Security Standard (PCI DSS)](https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss) v 3.2
 |  |  |
| [ ]  Federal Tax Information | * Internal Revenue Service Tax Information Security Guidelines for Federal, State and Local Agencies: [IRS Pub 1075](https://www.irs.gov/privacy-disclosure/safeguards-program)
 |  |  |
| [ ]  Personal Health Information  (PHI) | * Health Insurance Portability and Accountability Act of 1996: [HIPAA](https://www.hhs.gov/hipaa/for-professionals/privacy/index.html)
* The Health Information Technology for Economic and Clinical Health Act [HITECH](https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html)
* [Code of Federal Regulations 45 CFR 95.621](https://www.govinfo.gov/app/collection/cfr/2017/title45)
 |  |  |
| **Type of Data** | **Applicable State & Federal****Standards, Policies, and Laws** | **Comply** | **Vendor’s Description****of Compliance** |
| [ ]  Affordable Care Act  Personally Identifiable  Information (PII) | * Internal Revenue Service Tax Information Security Guidelines for Federal, State and Local Agencies [IRS Pub 1075](https://www.irs.gov/privacy-disclosure/safeguards-program)
* Minimum Acceptable Risk Standards for Exchanges [MARS-E 2.0](https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/)(Scroll down the page)
 |  |  |
| [ ]  Medicaid Information | * Medicaid Information Technology Architecture [MITA3.0](https://www.medicaid.gov/medicaid/data-and-systems/mita/mita-30/index.html)
* [Code of Federal Regulations 45 CFR 95.621](https://www.govinfo.gov/app/collection/cfr/2017/title45)
 |  |  |
| [ ]  Prescription Information | * [State law on the Confidentiality of Prescription Information](http://legislature.vermont.gov/statutes/section/18/091/04631)
 |  |  |
| [ ]  Student Education Data  | * Family Educational Rights and Privacy Act:  [FERPA](http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html)
 |  |  |
| [ ]  Personal Information from  Motor Vehicle Records | * [Driver’s Privacy Protection Act](https://www.congress.gov/bill/103rd-congress/house-bill/3355/text) (Title XXX) (“DPPA”) 18 U.S.C. Chapter 123, §§ 2721 – 2725
 |  |  |
| [ ]  Criminal Records | * Criminal Justice Information Security Policy:  [CJIS](https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view)
 |  |  |

**4.6 State of Vermont Cybersecurity Standard Update 2023-01**

Vendor shall certify by checking the box below the Solution shall not include, incorporate, rely on, utilize or be supported by any products or services subject to the limitations provided under State of Vermont Cybersecurity Standard Update 2023-01, which Contractor acknowledges has been provided to it, and is available on-line at the following URL: <https://digitalservices.vermont.gov/cybersecurity/cybersecurity-standards-and-directives>

[ ]  Contractor hereby certifies that in connection with the Request for Proposal, **none** of the applicable products or services will be included in or used to support State systems in a manner prohibited under the Standard.

## **Part 5: Implementation/Project Management Approach**

1. Describe the approach you would recommend for project managing this engagement.
2. Provide a list of the standard project management deliverables that you would normally produce for this type of engagement.
3. **Provide a proposed list of project phases, major milestones, and an implementation timeline. Label this Attachment #4.**
4. What types of difficulties have other clients experienced with implementation of the proposed solution?
5. Describe the experience and qualifications of the Project Manager you would offer as the resource for this engagement. **Provide a copy of their resume and label** **it Attachment #5.**

**Part 6: Technical Services**

1. Describe the technical services included in your proposal (e.g., business analysis, configuration, testing, implementation, etc.).
2. Provide a list of the standard deliverables for the technical services described above.
3. Provide a description of the roles/services/tasks the State will be expected to cover as part of this engagement. Describe any additional roles/services/tasks that are optional but would be beneficial for the State to provide.
4. Describe your typical conversion plan to convert data from existing systems to your proposed solution (if applicable).
5. Describe **and attach your typical Implementation Plan (label** **it Attachment #6)**, which shall include planning for the transition to maintenance and operations.
6. Describe the experience and qualifications of the technical resources proposed for this engagement. **Provide their resume(s) and label them Attachment #7.**
7. Describe the training that is included in your proposal.
8. Describe the system, administrator, and/or user documentation that is included in your proposal.

**Part 7: Maintenance and Support Services**

1. Provide answers to the questions below regarding your company’s Maintenance and Support Services:

|  |  |
| --- | --- |
| **Questions** | **Vendor Response** |
| **Service:  Customer Phone &/or Email Support** |
| What is the method for contacting technical support? |  |
| What are the hours of operation for support? |  |
| What is the turnaround time for responses? |  |
| What is the escalation process for support issues? |  |
| Who comprises the support team and what are their qualifications? |  |
| Define your response resolution metrics and how you capture and report them. |  |
| **Service:  Incident/Security Breach Notification and Process** |
| Describe your identification and notification process for security breaches. |  |
| **Service:  Data Management** |
| Describe how data is stored, retained and backed-up (including frequency). |  |
| **Service:  Hosting** |
| Describe the hosting service and associated service levels. |  |

|  |  |
| --- | --- |
| **Questions** | **Vendor Response** |
| **Service:  Scheduled Maintenance/Downtime** |
| What is the frequency of scheduled maintenance and downtime? |  |
| What is the notification process for scheduled maintenance and downtime? |  |
| Describe how “maintenance” updates are tested with customers prior to installing them in their live environments.  |  |
| **Service:  System Upgrades** |
| Are software upgrades provided as part of the software support contract?  |  |
| Describe your software upgrade process. |  |
| How often are new versions released? |  |
| Is documentation and training provided for system upgrades?  |  |
| Are there additional costs for upgrades and/or new releases? |  |
| Describe how and when the State will have an opportunity to test system upgrades/releases prior to live installation. |  |
| Describe how the State will validate post installation and how changes will be backed out in the event that a problem is encountered. |  |

|  |  |
| --- | --- |
| **Questions** | **Vendor Response** |
| **Service:  Bug Fixes and Minor Enhancements** |
| Describe the frequency and process for providing, testing, and installing bug fixes and minor enhancements. |  |
| **Service:  Disaster Recovery** |
| Describe the disaster recovery services included in this proposal for any non-state hosted services. |  |
| What is your standard RPO and RTO? |  |
| Describe the plan your company has in place for its own disaster recovery of any sites that may be involved in support of this proposal. |  |

1. Describe any other services not mentioned in the above list that are included in your standard Service Level Agreement (SLA) and **include a copy of your SLA with your response to this RFP. Label the SLA Attachment #8.**

The State’s minimum Service Level Agreements (SLAs) for the Solution are documented in the table below. Confirm if you will be able to meet the SLAs, and if not, provide a detailed explanation.

| **Service Area** | **Minimum SLA** | **Bidder Response** |
| --- | --- | --- |
| System Availability | * The acceptable amount of availability per month is 99.99% outside of designated maintenance windows for production environments.
 |  |
| System Availability | * The acceptable availability per month for non-production environments is 99.90% outside of designated maintenance windows.
 |  |
| System Responsiveness | The acceptable response time for user requests is 2 seconds, determined by calculating the time between when the request traverses into the solution and when the request traverses out. |  |
| System Responsiveness | Production environments\*:* RTO = 4 hours

All non-production environments\*:* RTO = 8 hours

Production environments\*:* RPO = 6 hours

All non-production environments\*:* RPO = 12 hours

\* If your proposed solution has concerns with meeting these metrics, please identify those concerns and any resulting cost variances, as well as any recommendations for State consideration. |  |
| Incident Response  | A one-hour response time during the Hours of Service for financial issues and outages that impact the normal operation of the system. |  |
| Incident Response | Same day resolution for data transmission errors and login issues during the hours of service. |  |
| Incident Notification and Restoration | Severity Level 1\* Incidents:* Restoration Start Time: Within 30 minutes
* Restoration Time: Within 4 hours
* Initial Notification: Within 30 minutes of identification
* Status Update Notifications: Every 1 hours
* Post 24-hour Status Update Notifications: Daily at the end of each business day

Severity Level 2\*\* Incidents:* Restoration Start Time: Within 60 minutes
* Restoration Time: Within 24 hours
* Initial Notification: Within 60 minutes of identification
* Status Update Notifications: Every 1 hours
* Post 24-hour Status Update Notifications: Daily at the end of each business day
 |  |
| Root Cause Analysis/Debrief | Vendor shall follow the CMS Guidance for Performing Root Cause Analysis with Performance Improvement Projects documentation which can be found at: <https://www.cms.gov/medicare/provider-enrollment-and-certification/qapi/downloads/guidanceforrca.pdf> .  |  |
| Root Cause Analysis/Debrief | Root Cause Debrief document must be uploaded to a designated OCS manager within five business days of incident closure. |  |
| Root Cause Analysis/Debrief | Root Cause Analysis status must be uploaded to the “knowledge repository” within twenty (20) business days of incident closure. |  |

\* “Severity Level 1” means production system down or a complete loss of service, the customer’s business operations are halted, or a critical system failure that impacts the entire user community and no workaround is possible. Ex. Inability for all users to login to a production environment, confirmed security breach, or day 0 virus/worm that results in a complete loss of service, critical services are mostly unavailable or not accessible to the majority of State operations, affecting a majority group or groups of people performing a critical business function.
\*\*“Severity Level 2” means service is degraded, resulting in a loss of major functions for a substantial portion of the customer’s user community. The customer’s business operations are severely limited though the customer may do some work. A workaround may be possible but is determined not feasible. Ex. Inability to access a production or non-production environment, Incidents having labor intensive workarounds and inefficient for the State, affects one or more groups of people performing a critical business function.

1. Describe how adherence to your service levels is measured and what remedies you would provide the State when performance doesn’t meet the standard?

## **Part 8: Pricing**

Submit pricing for your proposed solution in the table below. Fill in only the lines that are applicable to your proposal in the appropriate columns. If the line item is not applicable, enter N/A in the first column and leave the remaining columns in that row blank. **Insert lines for additional costs if needed, but do not delete or rename any lines in the Table**. You may provide your own detailed pricing schedule as a supplemental attachment as well.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Cost Type** | **Included in Solution** **(Yes, No or N/A)** | **Included in Convenience Fees****(Yes or No)** | **One Time/ Implementation Cost $** | **Recurring Cost $** | **Recurring Cost Basis (i.e., monthly, per payment)** |
| **Software** |  |  |  |  |  |
| Enterprise Application: License Fees |  |  |  |  |  |
| Maintenance &/or License Fee Add-Ons  |  |  |  |  |  |
| Subscription cost |  |  |  |  |  |
| Storage Limitations and/or Additional Fees |  |  |  |  |  |
| Database Software: License Fees |  |  |  |  |  |
| Middleware Tools: License Fees |  |  |  |  |  |
| Operating System Software: License Fees |  |  |  |  |  |
| Upgrade Costs for Later Years |  |  |  |  |  |
| Support and Maintenance Fees |  |  |  |  |  |
|  |  |  |  |  |  |
| **Implementation Services** |  |  |  |  |  |
| Project Management |  |  |  |  |  |
| Requirements  |  |  |  |  |  |
| Design (Architect Solution) |  |  |  |  |  |
| Development (Build, Configure or Aggregate)/ Testing |  |  |  |  |  |
| System Testing |  |  |  |  |  |
| Defect Removal |  |  |  |  |  |
| Implement/Deploy or Integrate |  |  |  |  |  |
| Quality Management |  |  |  |  |  |
|  |  |  |  |  |  |
| **Implementation Services Continued** |  |  |  |  |  |
| Training |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| **Telecom** |  |  |  |  |  |
| Bandwidth |  |  |  |  |  |
|  |  |  |  |  |  |
| **Hardware** |  |  |  |  |  |
| Computing Hardware  |  |  |  |  |  |
| Storage and Backup Hardware |  |  |  |  |  |
| Network Hardware |  |  |  |  |  |
| Facilities/Data Center |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| **Hosting** |  |  |  |  |  |
| Hosting Fees |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| **Kiosks / Point-of-Sale Options** |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. Describe any assumptions you have made in relation to the above cost and pricing information.
2. Provide pricing information for any volume discounts that are available based on the number of software licenses purchased or support years purchased.
3. Provide pricing for any Functional Requirements marked as “C” (feature is not available in the core solution but can be provided with customization).
4. Provide specific Convenience Fees for the following types of payments, and please indicate how these convenience fees are paid: i.e., per payment, per employee (for Employer payments), paid at time of processing, in addition to the child support funds, etc.:
	1. Credit Card
	2. Debit Card
	3. PayPal Credit
	4. PayPal
	5. Venmo
	6. Apple Pay
	7. Google Pay
	8. Cash at Kiosk
	9. ACH / e-check
	10. Other

**Part 9: Terms and Conditions**

In deciding which Respondent/s to shortlist the State will take into consideration each Respondent’s willingness to meet the State’s terms and conditions. Indicate any objections or concerns to our stated terms and conditions in the RFP or any of the exhibits, addendums or attachments including **Attachment C**. Add lines to the table below as needed.

**Important:** Bidder will be bound to all terms and conditions stated in the State’s RFP, exhibits, attachments, and/or addendums except and then only to the extent specifically set forth in the table below, and only if and to the extent expressly agreed and incorporated in writing in a resulting contract. Note that exceptions to contract terms may cause rejection of the proposal.

|  |  |  |
| --- | --- | --- |
| **Clause Location** | **Concern** | **Proposed Verbiage** |
| [indicate RFP, exhibit, attachment or addendum, section & page number] | [briefly describe your concern about this clause] | [describe your suggested alternative wording for the clause or your solution] |
| [indicate RFP, exhibit, attachment or addendum, section & page number] | [briefly describe your concern about this clause] | [describe your suggested alternative wording for the clause or your solution] |
| [indicate RFP, exhibit, attachment or addendum, section & page number] | [briefly describe your concern about this clause] | [describe your suggested alternative wording for the clause or your solution] |
|  |  |  |
|  |  |  |

**Part 10: CERTIFICATE OF COMPLIANCE/Authorized Company Signature**

**For a bid to be considered valid, this Part 10 must be completed in its entirety, executed by a duly authorized representative of the bidder, and submitted as part of the response to the proposal.**

1. **NON COLLUSION:** Bidder hereby certifies that the prices quoted have been arrived at without collusion and that no prior information concerning these prices has been received from or given to a competitive company. If there is sufficient evidence to warrant investigation of the bid/contract process by the Office of the Attorney General, bidder understands that this paragraph might be used as a basis for litigation.
2. **CONTRACT TERMS:** Bidder hereby acknowledges that is has read, understands and agrees to the terms of this RFP, including Attachment C: Standard State Contract Provisions, and any other contract attachments included with this RFP.
3. **Worker Classification Compliance Requirement:** In accordance with Section 32 of The Vermont Recovery and Reinvestment Act of 2009 (Act No. 54), the following provisions and requirements apply to Bidder when the amount of its bid exceeds $250,000.00.

**Self-Reporting.** Bidder hereby self-reports the following information relating to past violations, convictions, suspensions, and any other information related to past performance relative to coding and classification of workers, that occurred in the previous 12 months.

|  |  |  |
| --- | --- | --- |
| **Summary of Detailed Information** | **Date of Notification** | **Outcome** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Subcontractor Reporting.** Bidder hereby acknowledges and agrees that if it is a successful bidder, prior to execution of any contract resulting from this RFP, Bidder will provide to the State a list of all proposed subcontractors and subcontractors’ subcontractors, together with the identity of those subcontractors’ workers compensation insurance providers, and additional required or requested information, as applicable, in accordance with Section 32 of The Vermont Recovery and Reinvestment Act of 2009 (Act No. 54), and Bidder will provide any update of such list to the State as additional subcontractors are hired. Bidder further acknowledges and agrees that the failure to submit subcontractor reporting in accordance with Section 32 of The Vermont Recovery and Reinvestment Act of 2009 (Act No. 54) will constitute non-compliance and may result in cancellation of contract and/or restriction from bidding on future state contracts.

1. **Executive Order 05 – 16: Climate Change Considerations in State Procurements Certification**

**Bidder certifies to the following (Bidder may attach any desired explanation or substantiation. Please also note that Bidder may be asked to provide documentation for any applicable claims):**

* 1. Bidder owns, leases or utilizes, for business purposes, space that has received:
* Energy Star® Certification
* LEED®, Green Globes®, or Living Buildings Challenge℠ Certification
* Other internationally recognized building certification:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Bidder has received incentives or rebates from an Energy Efficiency Utility or Energy Efficiency Program in the last five years for energy efficient improvements made at bidder’s place of business. Please explain:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. Please Check all that apply:

* Bidder can claim on-site renewable power or anaerobic-digester power (“cow-power”). Or bidder consumes renewable electricity through voluntary purchase or offset, provided no such claimed power can be double-claimed by another party.
* Bidder uses renewable biomass or bio-fuel for the purposes of thermal (heat) energy at its place of business.
* Bidder’s heating system has modern, high-efficiency units (boilers, furnaces, stoves, etc.), having reduced emissions of particulate matter and other air pollutants.
* Bidder tracks its energy consumption and harmful greenhouse gas emissions. What tool is used to do this? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Bidder promotes the use of plug-in electric vehicles by providing electric vehicle charging, electric fleet vehicles, preferred parking, designated parking, purchase or lease incentives, etc.
* Bidder offers employees an option for a fossil fuel divestment retirement account.
* Bidder offers products or services that reduce waste, conserve water, or promote energy efficiency and conservation. Please explain:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Please list any additional practices that promote clean energy and take action to address climate change:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**PART 11 SUBCONTRACTOR REPORTING FORM**

**This form must be completed in its entirety and submitted prior to contract execution and updated as necessary and provided to the State as additional subcontractors are hired.**

The Department of Buildings and General Services in accordance with Act 54, Section 32 of the Acts of 2009 and for total project costs exceeding $250,000.00 requires bidders to comply with the following provisions and requirements.

Contractor is required to provide a list of subcontractors on the job along with lists of subcontractor’s subcontractors and by whom those subcontractors are insured for workers’ compensation purposes. Include additional pages if necessary. This is not a requirement for subcontractor’s providing supplies only and no labor to the overall contract or project.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Subcontractor** | **Insured By** |  | **Subcontractor’s Sub** | **Insured By** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Date:

Name of Company: Contact Name:

Address: Title:

Phone Number:

E-mail: Fax Number:

By: Name:

Failure to adhere to Act 54, Section 32 of the Acts of 2009 and submit Subcontractor Reporting: Worker Classification Compliance Requirement will constitute non-compliance and may result in cancellation of contract and/or forfeiture of future bidding privileges until resolved.

Send Completed Form to:

Office of Purchasing & Contracting

133 State Street, 5th Floor

Montpelier, VT 05633-8000

I am authorized to submit a proposal to the State of Vermont in response to this RFP on behalf of my organization. The information provided as part of my organization’s response is a true and accurate representation of my organization’s ability to meet the State of Vermont’s business needs as expressed in this RFP.

|  |  |
| --- | --- |
| **Signature:** |  |
| **Full name:** |  |
| **Title:** |  |
| **Company:** |  |
| **Date:** |  |