**Appendix 5 – Bidder Response Form**



**State of Vermont Bidder Response Form**

**Request for Proposal Name: Mainframe Outsourcing**

**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:

**Roland Ortiz,** Technology Procurement Administrator

State of Vermont

Office of Purchasing & Contracting

E-mail Address: **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.
2. Please provide information that communicates your experience and expertise in providing mainframe outsourcing services (e.g., number of customers in public and private sector, years offering mainframe outsourcing services, service differentiators, etc.…).
3. 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 and architectural specification of the technology solution you are proposing considering the scope of services section of the RFP and State of Vermont’s current state described in Appendix 1, 2, and 3. Please note that the State is not looking to engage in any significant application refactoring to accommodate mainframe hardware or software changes. Mandatory or elective changes relative to the current state should be justified in the response to this question. The State will look at application refactoring to accommodate changes that require more than 16 hours from the State’s Application M&O team, inclusive of requirement and technical design documentation, coding, and smoke testing as significant application refactoring. If the Vendor system/software solution supports multiple customers on the same infrastructure, describe how the State’s data is isolated such that other non-State customer users are prevented from accessing the State’s data.
2. Provide a high-level description of the following aspects of the solution you are proposing:
	1. The standard, default features and functions of the solution:
	2. The standard, default software licensing requirements for the solution:

	It is required that the vendor will be providing all required IBM software in its pricing proposal.

	It is preferred that the vendor provide all required third party software licenses (i.e., non-IBM software). See section 3.3.1 in RFP for more context.
	3. The standard performance levels:
		* Hours of system availability
		* System response time
		* Maximum number of concurrent users
		* Other relevant performance level information
3. List the total number of installations (i.e. mainframe hosting services) in the last 4 years by the year of installation.
4. Have you implemented similar solution for other government entities? If so, what specific challenges did you face during the implementation?
5. **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.**
6. **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.**
7. Does your proposed solution include any warranties? If so, describe them and provide the warranty periods.
8. Describe any infrastructure, equipment, network or hardware *required* to implement and/or run the solution.
9. What is your recommended way to host this solution?

## **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 provided with customization.

**N** - Feature is not available.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID #** | **Functional Requirement Description** | **Availability** | **Vendor Comments** |
| **1 Operational** |
| A | Vendor must agree to all specified vendor roles and responsibilities for both AHS\AOT and VDOL mainframe and supported applications listed in Appendix 4. |  |  |
|  |  |  |  |
| **2 Data Center** |
| A | The solution(s) must provide adequate CPU processor specifications (memory, channels to peripherals, OSA connectivity) that meet our SLA requirements and that provides a user experience comparable to the State’s current mainframe solutions. See Appendix 1, 2, and 3 for current state details. |  |  |
|  |  |  |  |
| **2 Reporting** |
| A | Provide all mainframe environmental reports, including resource consumption reports, that allow the State to understand the health and performance of mainframe solutions. A list and specification of these reports to be completed with the State during implementation.  |  |  |
| B | For the AHS\AOT mainframe solution, the vendor must provide one or more reports that detail relative mainframe resource consumption for each Agency\Department down to the specific program level (e.g., SNAP, OCS, LTC, etc..).  |  |  |
| C | The vendor shall produce one or more reports that will allow the State to assess vendor SLA performance. |  |  |
| D | Provide ad hoc reports (e.g., during IRS audit various reports are needed to address specific questions) on an as needed basis as part of base hosting support.  |  |  |
| **4 Integrations**  |
| A | Vendor shall support all existing system interfaces – listed in Appendix 6.  |  |  |
| B | Vendor shall integrate with the State’s issue and service request ticketing systems (currently iVanti) and use it as primary means to track issues and service request with the State. |  |  |
| C | Vendor shall provide an extensible solution that can integrate into the State’s current and future systems and solutions.  |  |  |
|  |  |  |  |

## **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 provide for back-up and disaster recovery models and plans as needed for the solution.  |  |  |
| H3 | Any hosting provider will abide by ITIL best practices for change requests, incident management, problem management and service desk.  |  |  |
| H4 | Service Providers will describe the production support and transition approach and methodology used for transitioning out solutions. |  |  |
| H5 | Service Providers will provide a Transition-Out Plan for approval by the State prior to production support commencement. The Plan will contain transition task descriptions, an organization chart, and job descriptions for all support staff. The State will provide electronic notice if it wishes this transition to be evaluated or enacted. |  |  |
| H6 | Service Providers will incorporate the production support and transition approach into a comprehensive Production Support and Transition-In Plan complying with Solutions architectural design that describes solution and transition support over to the entity responsible for on-going production operations and support. |  |  |
| H7 | Solutions will provide tooling to support the Extract-Transform-Load (ETL) process that involves: Extracting data from data sources. Transforming to fit business needs (which can include quality levels). - Loading into the target data store. - Caching: The ability to cache federation results and various subsets of the source data to improve performance in situations where source data volumes are large; therefore, retrieving all data required for integration directly from the source is not feasible. |  |  |
| H8 | Solutions will support access from multiple channels and devices. |  |  |
| H9 | The solution provider must support Application-to-Application interfaces/integrations that must be quick and efficient, thus not negatively impacting user experience. |  |  |
| H10 | Service provider will collect performance and capacity metrics (including monitoring alerts or incidents) and will conduct analysis of metrics to identify and remedy any possible capacity issues. |  |  |
| H11 | Once the capacity plan has been approved, changes to the capacity plan will be under the control of the change management process. |  |  |
| H12 | Hosting Service provider will establish workload management practices to distribute the batch workload evenly across system resources and across the daily, weekly, and monthly production schedules, including scheduling of batch jobs, execution of reports, and all other business activity that impacts system performance. This will be detailed within the capacity plan. |  |  |
| H13 | The following capacity management KPIs/metrics will be tracked and reported by the hosting service provider: Total incidents, with cause of capacity, number of emergency changes related to capacity incidents, comparison of capacity forecasts against actual consumption. Service provider will add KPIs to the above list, as requested by the State of Vermont (SOV) in support of the business and continuous improvement. |  |  |
| H14 | System will support concurrent internal and external users as per contract. This will be tested using load testing prior to go-live and periodically after major release as part of the capacity plan. |  |  |
| H15 | Solutions will provide the ability to optimize individual queries and support parallelizing a query to run on multiple CPUs at the same time to increase performance. |  |  |
| H16 | "If required, the Solution Provider will produce a Capacity Management Plan. The document should include the following- A description of the scope and objectives of the plan, such as the systems, services, processes, and stakeholders involved.- A summary of the current state of the systems and services, such as their performance, availability, reliability, scalability, and security.- A forecast of the future demand and growth of the systems and services, based on historical data, trends, projections, and business plans.- A gap analysis that identifies the potential risks and issues that may arise from the mismatch between the current and future capacity needs.- A strategy and action plan that defines the actions and resources needed to close the gaps and ensure adequate capacity for the systems and services.- A set of metrics and indicators that will be used to monitor and report on the progress and effectiveness of the plan.- A review and update process that ensures the plan is regularly evaluated and revised to reflect changing needs and circumstances." |  |  |
| H17 | Service Provider will deploy capacity and performance monitoring tools that allow servers, networks, databases, storage, applications, data center infrastructure to scale and shift workloads on-demand without any user perceived interruption. |  |  |
| H18 | Solutions will support indexing technology (multiple types of indexing will be available to tune performance of SQL statement). |  |  |
| H19 | Solutions will support high performance and scalability, including the following characteristics: High performance for large rule bases (more than 20,000 rules). Ability to share rule sets across multiple engines. Dynamic and static execution versions for performance. Multiple, cross-platform support. Segmented repositories. Pre-built rule paths. Rule pre-fetch to memory. Parallel rule search. Ability to compile rule sequences into base languages, e.g., C++, Java and C. |  |  |
| H20 | The solution must have a monitoring and logging mechanism to track and report the performance metrics and errors. |  |  |
| H21 | The solution must support multiple browsers and devices with different screen sizes and resolutions. |  |  |
| H22 | If necessary and required for the solution, Service provider will specify IP addresses to route to service provider’s data center(s), including those that should be routed over the Transaction Link or Management Link, if required. |  |  |
| H23 | The solutions to have comprehensive and flexible data source connectivity tools through adapters. The tools must support a range of source types, including non-solution database and legacy databases, packaged applications, web services, semi-structured and unstructured data, and XML structures. This NFR ensures that the system can access and utilize data from different sources, enabling efficient and effective data processing and management. |  |  |
| H24 | Solutions will provide real-time interfaces to transfer data between solution and existing State of Vermont (SOV) systems, e.g., the Eligibility Rules Engine, SOV Medicaid systems, Case Management systems, Identity Access Management systems, SERFF, HIOS, Federal Data Services Hub, external systems, databases and financial systems. |  |  |
| H25 | SaaS Service Providers will comply with the Multi-tenancy Service Provider Expectations Document and note any Service Provider system support service expectations that are not covered. |  |  |
| H26 | Solutions will define what is the level and complexity of data transformations required to support the information exchange needs between applications |  |  |
| H27 | The solution provider will meet requirements as identified in the corresponding HL7 FHIR Implementation Guides (IG) for Blue Button, PDEX and others as apropos and these Blue Button IGs will be considered the standards needed for 3rd parties to access the data. |  |  |
| H28 | Solutions will support the industry standards for messaging, receiving and sharing data and interfaces relevant to health and human services organizations including, but not limited to: FHIR Version 4.0 and Electronic Data Interchange (EDI) X12 healthcare format. The versioning for these products must be maintained to meet the evolving requirements of the State of Vermont 's (SOV's) CMS and ONC and any other bodies that dictate these standards. |  |  |
| H29 | Solutions will include the following types of transformation: Simple transformations, e.g., data-type conversions, string manipulations and simple calculations. Moderate-complexity transformations, e.g., lookup and replace operations, aggregations, summarizations, deterministic matching and management of slowly changing dimensions. Higher-order transformations, e.g., sophisticated parsing operations on free-form text and rich media. Facilities for developing custom transformations and extending packaged transformations. |  |  |
| H30 | Solutions will have the capability to support the global identification, linking and/or synchronization of client and provider information across heterogeneous data sources through semantic reconciliation of master person index (MPI) data. |  |  |
| H31 | Solutions will support authoring and management of solution data. Solutions will provide a flexible and comprehensive workflow-based capability that can be used to create and maintain workflows supporting solution data maintenance across the multiple source solutions. |  |  |
| H32 | The software shall support backward compatibility with at least two previous versions of the software, ensuring that users can upgrade without losing any important data or functionality. |  |  |
| H33 | The software shall support easy data migration from the current version to future versions of the software, ensuring that users can upgrade without losing any important data or functionality |  |  |
| H34 | The software shall be able to handle large volumes of data and traffic, and support the scaling of resources to meet the demands of the environment in which it operates. |  |  |
| H35 | Solutions will have the ability to support varying message payloads, ranging from individual transactions to large files (more than 1GB) containing multiple transactions. The SOA solution will be configured to appropriately manage these varying types of message construction and size through a common set of components. Where possible, solutions will error on the side of individual transactions per message to simplify the message management, routing, and database recovery needs. |  |  |
| H36 | Solution will define the requirement for all software to support data integration with other systems |  |  |
| H37 | Solutions running on shared Infrastructure will support reorganization of database/index/configuration online without the need for the solution to shut down. |  |  |
| H38 | Healthcare-related solutions will at a minimum support the following standards, Integrating the Health Enterprise (IHE). Cross-Enterprise Document Sharing (XDS, XDS.b). Cross-Community Access (XCA). Health Level Seven (HL7), Fast Healthcare Interoperability Resources (FHIR), EDI X12N, Digitial Imaging and Communications in Medicine (DICOM), Continuity of Care Document (CCD) C32 profile (AHS ONC Direct Project). |  |  |
| H39 | The solution must support all web browser with a market share in the United States of America greater than 3%, as indicated by gs.Statcounter.com |  |  |
| H40 | The proposed solutions must allow for the migration of information such as case file data, from the State's mainframe system to shared application and database systems to ensure its availability. |  |  |
| H41 | Complete Disaster Recover Testing four times per year including documentation of test results for the VDOL Mainframe solution. |  |  |
| H42 | Complete Disaster Recover Testing annually and providing the State with the test results for the AHS\AOT Mainframe Solution |  |  |
| H43 | Maintain Internet bandwidth to support at least a 95% monthly average utilization of 8 Mbps.  |  |  |
| H44 | Maintain redundant VPN network connection with the State’s on-premise data center and it’s Azure Cloud instance.  |  |  |

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

**4.2 Application Solution**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID #** | **Non-Functional Requirement Description** | **Comply** | **Vendor’s Description of Compliance**  |
| A1 | The solution provider will provide an Availability Plan for the 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. |  |  |
| A2 | The solution provider will provide Service Continuity Management for the Production Environment following a declared Disaster. |  |  |
| A3 | The solution provider will conduct an implementation readiness review at least ten days prior to production cutover. |  |  |
| A4 | The solution provider will inform the State when it plans to use regular maintenance periods instead of a different time slot allocated for the State-specific Release Management tasks. |  |  |
| A5 | The solution provider will offer Hyper-care support must be provided that includes a stabilization period after go-live and details ongoing support services, including production support, application maintenance, and enhancements. |  |  |
| A6 | As part of Monitoring Services, The solution provider will use information collected by tools to monitor use, performance and availability of the The solution provider Programs and to resolve service requests. |  |  |
| A7 | In advance of any release or changes the solution provider will produce for the State the following: Change release documentation: that describes the changes made to the solution such as new features, bug fixes, and enhancements.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.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.  |  |  |
| A8 | The solution provider must support hardware and network load balancing technologies for high availability and maintenance. |  |  |
| A9 | The solution must support independent deployment of modules, allowing for more frequent updates and reducing the risk of system-wide downtime during maintenance. |  |  |
| A10 | The solution must support monitoring and logging of system events and errors to facilitate root cause analysis and troubleshooting. |  |  |
| A11 | The solution must support automated analysis tools for identifying and reporting on issues such as code quality, security vulnerabilities, and performance bottlenecks. |  |  |
| A12 | The solution must support the addition of new functionality, modules, and components without requiring extensive modifications to the existing system |  |  |
| A13 | The solution must support the modification of existing functionality, modules, and components without introducing unintended consequences or side effects. |  |  |
| A14 | The solution must support version control and rollback capabilities to facilitate quick and easy reversions in case of errors or issues with new updates. |  |  |
| A15 | The solution must support automated testing, with clear and well-defined test cases and test data. |  |  |
| A16 | The solution must support the use of testing and simulation tools to facilitate unit testing, integration testing, and performance testing. |  |  |
| A17 | The solution architecture will allow for transaction tracking and review throughout the system for auditing, error diagnosis, and performance management purposes. |  |  |
| A18 | The Implementation Plan will include information on technical challenges, deployment schedule phasing. The Implementation Plan will deliver solutions that include a significant portion of the technical infrastructure and application early in the schedule, without compromising the quality or inherent security of the solution. This will also validate the design and architecture and expose technically challenging areas of the project as soon as possible. Deliver customized functionality to the State in incremental pieces that are in logical business application sequence. |  |  |
| A19 | 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. |  |  |
| A20 | Solutions will include a workflow tool to support the records management process. |  |  |
| A21 | Solutions will support reporting requirements either natively or integrate with other reporting tools to provide reporting. |  |  |
| A22 | Solutions will provide access to standardized reporting, ad hoc queries, and data visualization. |  |  |
| A23 | 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 |  |  |
| A24 | 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. |  |  |
| A25 | Solutions will provide support for web content management solution that is robust, scalable, and provides workflow management. |  |  |
| A26 | 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. |  |  |
| A27 | 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. |  |  |
| A28 | Solutions will provide time-based content expiration and version management capabilities. |  |  |
| A29 | Solutions will provide support for full text search. |  |  |
| A30 | 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. |  |  |
| A31 | The solution must support multiple languages, currencies, time zones, and regional settings for different markets and users. |  |  |
| A32 | The solution must learn from the feedback and data collected from the customers and users by analyzing, interpreting, reporting, etc. them. |  |  |
| A33 | The solution must support multiple versions of the service for different customer segments or scenarios by using version control systems and techniques. |  |  |
| A34 | The solution must provide transparency and accountability for the service by documenting and reporting the activities, outcomes, decisions, etc. of the service. |  |  |

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

**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 | The Contractor must collaborate with the State to provide a Risk Management Plan (RMP), for all phases of the overall system implementation and operations project, that at a minimum, complies with industry project management standards, includes a Comprehensive Risk Assessment and Risk Mitigation Plan  |  |  |  |
| S2 |  The Contractor must ensure the system(s) is compliant upon Operational Go‑Live and remains compliant with applicable State and Federal regulations and standards contained in National Institute of Standards and Technology (NIST) Publication 800-53 current revision and the current version of IRS Pub 1075, proven through independent third-party production security controls assessment. This assessment must be conducted at a minimum annually, at no cost to the State and by a State‑approved third party that maintains no financial or controlling relationship with The Contractor. The Contractor must be responsible for modifications to remain compliant, including compensating controls to mitigate gaps. Additionally, the Contractor must generate documented assessment results and produce 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. |  |  |  |
| S3 |  The Contractor must review and update the risk mangement plan, risk assessment, and risk mitigation plan, at a minimum on an annual basis, in coordination with AHS and the assigned ADS Security Analyst. |  |  |  |
| S4 |  The Contractor must collaborate with the State to provide a System Security Plan (SSP) that, at a minimum, documents the State's plan to comply with State and Federal Security and Privacy rules. The State must approve the SSP and all associated artifacts, and must conduct audits/evaluations of the Plan established by The Contractor at least annually. |  |  |  |
| S5 |  The Contractor must ensure the System Security Plan enables the following processes and/or data collection activities to occur: a) Development and submission of a Statement on Standards for Attestation Engagements (SSAE) 18, Service Organization Control (SOC) 2 Type II Compliance Report from hosting provider(s)b) Development and maintenance of organizational information security policies c) Privacy Impact Analysis that identifies the data elements of the system that expose Vermont beneficiaries to potential privacy threats and the system controls in place to mitigate private data disclosure risks d) A security event notification process, event evaluation and escalation procedures, and security event response procedures e) A complete network diagram showing servers, printers, workstations, firewalls, intrusion prevention systems, network security device internet connections, and any other network connected device f) Documented firewall security standards and diagrams showing sufficient detail of data flows in and out of security boundaries; including items such as VPNs, subnets, ports and protocols g) A detailed plan for system log collection and monitoring h) An antivirus deployment/maintenance plan i) A software maintenance plan, including operation systems and third-party software updates j) An agreement that criminal background checks must be completed and passed by all employees prior to being allowed access to State data k) Procedures to limit access to information to those individuals who need such information for the performance of their job functions and ensuring that those individuals have access to only the information that is the minimum necessary for the performance of their job functions l) A description of how physical safety of data under its control must be protected using appropriate devices and methods, including alarm systems, locked files, guards, or other devices expected to prevent loss or unauthorized access to data m) A description of the steps taken to prevent unauthorized use of passwords, access logs, badges, or other methods designed to prevent loss of, or unauthorized access to, electronically or mechanically held data n) An agreement to comply with Health Insurance Portability and Accountability Act, (HIPAA) Privacy Rules (Federal regulations) as a Business Associate of the State.  |  |  |  |
| S6 |  The Contractor must ensure that the System Security Plan complies with State and Federal laws, rules, regulations, standards, and guidelines to include the following:a) NIST Publication 800-53, current revisionb) IRS Pub 1075, current revisionc) Federal Information Processing Standard (FIPS) 200d) The American Recovery and Reinvestment Act (ARRA)e) Title XIX of the Social Security Actf) Title II, Subtitle F, Sections 261 through 264 of the HIPAA, Pub. L. 104 191g) Health Insurance Portability and Accountability Act of 1996 (HIPAA)h) Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidelinesi) Health Information Technology for Economic and Clinical health Act (HITECH) of 2009j) Federal Information Security Management Act (FISMA) of 2002k) Safeguards for Protecting Federal Tax Returns and Return Information (26 U.S.C. § and related provisions)l) Social Security Administration (SSA) Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information With the Social Security Administration |  |  |  |
| S7 |  The Contractor must ensure the system(s) maintains compliance with current and future security, privacy, accessibility, and certification laws (State and Federal), regulations, policies, and guidelines relevant to system security, confidentiality, integrity, availability, and safeguarding of information, where any of these overlap, The Contractor must ensure that the system(s) must always strive to attain the more stringent policy. Contractor retains responsibility for all modifications to the system(s) to maintain compliance according to the terms and conditions of the resulting Contract. |  |  |  |
| S8 |  The Contractor must ensure the confidentiality, integrity, and availability of all regulatory data. Further, The Contractor must ensure the system supports integrity controls to guarantee that transmitted regulatory data is not improperly modified without detection. Any successful or unsuccessful attempts of modification of regulatory data must be reported to the State as part of a monthly summary report. |  |  |  |
| S9 |  The Contractor must notify the State within 30 minutes of their confirmation of an unauthorized attempt at modification of regulatory data. Upon discovery, the Contractor must validate the discovery within 14 business days. |  |  |  |
| S10 |  The Contractor must implement policies and procedures for guarding, monitoring, and detecting malicious software (e.g., viruses, worms, malicious code), implement controls based on trends, and report all discoveries to the State monthly. |  |  |  |
| S11 |  The Contractor must notify the State within 30 minutes of their confirmation of a malicious software attempt. |  |  |  |
| S12 |  The Contractor must notify the State within 30 minutes of their confirmation of an abnormal data behavior. The Contractor and the State must mutually define abnormal data behavior. |  |  |  |
| S13 |  The Contractor must propose, for State approval, and implement system controls to ensure system security during software program changes and promotion in any environment that contains regulatory data. The Contractor must report any successful security breaches during the software change or promotion. |  |  |  |
| S14 |  The Contractor must ensure that all applications are protected against unauthorized access per State and Federal guidelines. Additionally, all transmission lines and communications services and linkages between the data and each information system must always be secure from unauthorized access between each system, and the network. All attempts of unauthorized access must be reported to the State in a monthly summary report. |  |  |  |
| S15 |  The Contractor must notify the State within 30 minutes of their confirmation of a successful unauthorized access request. The Contractor must validate the discovery within 14 business days. |  |  |  |
| S16 |  The Contractor must monitor and provide State-approved metrics and reporting on system security, privacy, confidentiality, accessibility, and integrity on a monthly basis. |  |  |  |
| S17 |  The Contractor must notify the State within 30 minutes of their confirmation of a successful breach of system security. The Contractor must validate the discovery within 14 business days. |  |  |  |
| S18 |  The Contractor must maintain a Security Breach Response Team available 24 hours a day, 7 days a week and within 5 minutes of notification of an incident to respond to security violations and breaches (physical and electronic). This includes communications to a defined list of personnel at the State tied to the State's Continuity of Operations/Disaster Recovery (COOP/DR). State staff must be informed of response plan, including specific steps and time frames for resolution. |  |  |  |
| S19 |  The Contractor must initiate communications with State staff during a security incident that must be hourly and progressive. |  |  |  |
| S20 | The Contractor must collaborate with the State to define a comprehensive process for managing the Access Reporting component of the System Security Plan that applies to granting, monitoring, tracking, and storage of all user access. This plan must be maintained on an annual basis. |  |  |  |
| S21 | The Contractor must provide a State-approved, 508 compliant user-centered designed and intuitive interface for Security Administrators to grant, track, manage, and revoke access for individuals. System must also provide auditing capabilities for approved audit resources. |  |  |  |
| S22 | The Contractor must conduct a review of all access rights and update access rights quarterly or upon request of the State. Contractor must create a report listing all review activities and actions. All such documentation must be maintained a minimum of 10 years per regulatory retention requirements. |  |  |  |
| S23 | The Contractor must monitor and enforce all access criteria in accordance with State security access and management policies and provide a flexible security management solution capable of maintaining compliance with future State security access and management policies. |  |  |  |
| S24 | The solution will ensure secure network infrastructure that is self-contained and in its own security perimeter. In securing these perimeters, the Contractor will enforce the use of current and supported International Computer Security Association (ICSA) compliant firewalls, and/or similarly robust perimeter solutions provided through IaaS and PaaS cloud offerings. |  |  |  |
| S25 | 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. |  |  |  |
| S26 | The Contractor must maintain system and access log files for relevant systems and make them available to the State in accordance with mutually agreed upon auditing and security activities. These log files must contain a complete accounting of all activity for a given system. Contractor must provide State‑authorized Stakeholders access to all logs and provide the ability to perform ad hoc reporting. |  |  |  |
| S27 | The Contractor must design and execute security testing to prevent unauthorized access to the system (intrusion detection and vulnerability testing) on a quarterly basis and provide a report of all findings to the State within 10 business days. Any issues identified and reported to the State are to be resolved according to their respective SLA. |  |  |  |
| S28 | The Contractor must ensure all data is restricted to the United States. |  |  |  |
| S29 | The Contractor must ensure all levels of security, within the enterprise system(s) applications are in alignment with State policy, Federal guidance, and procedures. |  |  |  |
| S30 | The Contractor must provide a Data Classification Schema based on the current version of National Institute of Standards and Technology (NIST)Special Publication 800-53 data classification categories. The Contractor must also provide an Access Privilege Scheme to limit users' access based upon the defined data classification categories. |  |  |  |
| S31 | The Contractor must establish, enforce, document, communicate, and seek State approval of responsibilities, processes, and procedures for all usage types, in accordance with State and Federal standards and laws. |  |  |  |
| S32 | The Contractor must ensure system capabilities include NIST compliant role-based access control (e.g., add, update, read, delete) and how roles should be available in the system. Contractor must provide tools for identified State staff to define various roles. |  |  |  |
| S33 | The solution must ensure complete segregation of State data from other Contractor customers to prevent the access of State data from unauthorized parties. All access requests must be approved by designated State staff. The solution must comply with all court ordered or warranted requests for data access. |  |  |  |
| S34 | The solution must provide Internet security functionality to include the use of firewalls, intrusion detection/intrusion prevention (IDS/IPS), https, encrypted network/transport layer security (TLS), and security provisioning protocols such as transport layer security, and Internet protocol security (IPSEC), as well as provide data loss prevention tools (DLP) and use supported certificates. |  |  |  |
| S35 | The solution must implement and maintain a secure environment for both online and batch access to State data using a fully functional and documented security software package for all environments. This secure environment must include web application testing protocols, the use of code review software and secure file transfer meeting FIPS 140‑2 standards, or FIPS 140 standards as adopted by NIST, and enabling all reporting of testing and review activities available to the State. |  |  |  |
| S36 | The solution must encrypt data at rest, at transfer, and backed‑up data per FIPS 140‑2 Standards (FIPS 140-3 after September 21, 2026). |  |  |  |
| S37 | The solution must provide three types of controls to maintain data integrity:a) Preventive Controls: Controls designed to prevent errors and unauthorized events from occurringb) Detective Controls: Controls designed to identify errors and unauthorized transactions which have occurred in the systemc) Corrective Controls: Controls to ensure that the problems identified by the detective controls are corrected. These controls must be in place at all appropriate points of processing to comply with the current version of NIST standards. Should the solution not meet these standards, compensating controls, approved by the State, must be implemented. |  |  |  |
| S38 | The solution must contain a data definition for the Designated Record Set (DRS) that allows it to be included in responses to inquiries and report requests, as well as:a) Provide the ability to respond to an authorized request to provide a report containing the DRS for a given individualb) Ensure the system provides the capability to identify and note amendments to the DRS for a given individualc) All such documentation must be maintained a minimum of ten years in alignment with federal retention requirements. |  |  |  |
| S39 | The solution must:a) verify the identity of all users and denies access to invalid usersb) support a user security profile that controls user access rights to data categories and system functionsc) maintain a list of users and their security profiles, including updating security files with State-approved additions of new staff and changes to existing security profiles and staff terminationsd) provide multi-factor authentication (MFA) that is scalable and aligns with Federal guidelinese) Initially grant users accounts with no access rights and build each user’s security rights profile based on user role and approved security access. |  |  |  |
| S40 | The Contractor must designate a full‑time Compliance and Security officer to ensure and maintain compliance with federal standards. |  |  |  |
| S41 | The Contractor must provide, test, update, maintain, and submit, for State review and approval, Business Continuity (BC)/Disaster Recovery (DR) and Cyber Incident Response (CIR) Plans that are aligned to NIST CP-2 and IR-8, current verion of NIST-800-53, NIST 800-34; and meet all Federal and State standards, on an annual basis or more frequently as directed by the State, such as after a major system change that materially affects the BC/DR and CIR Plans. |  |  |  |
| S42 | The Contractor must perform annual (including pre-go-live) Business Continuity (BC)/Disaster Recovery (DR) and Cyber Incident Response (CIR) exercises. Exercises must include activities selected from the BC/DR and CIR Plans to verify the viability of each BC/DR and CIR Plan in accordance with NIST CP-4 and IR-8 standards. Exercises must also be performed after major system changes as required by the State. The Contractor must document all testing activities and report to the State instances where appropriately trained personnel were unable to complete the necessary recovery procedures. The Contractor must adjust contingency and training plans to correct the identified plan deficiencies and present updates to the State for approval. |  |  |  |
| S43 | The Contractor must provide annual test reports to the State within 10 business days of exercise, Business Continuity (BC)/Disaster Recovery (DR) and Cyber Incident Response (CIR) Plan reports within one business day of incident, and BC/DR and CIR Plan updates within one business day of identified deficiency. |  |  |  |
| S44 | The Contractor must evaluate systems and business processes in collaboration with the State for criticality and necessity to determine appropriate return to operations time frames during development of both the initial and ongoing Business Continuity (BC)/Disaster Recovery (DR) and Cyber Incident Response (CIR) Plans |  |  |  |
| S45 | In coordination with the State, the Contractor must provide training to Contractor staff and State identified Stakeholders on the execution of the Business Continuity (BC)/Disaster Recovery (DR) and Cyber Incident Response (CIR) Plans a minimum of 20 business days prior to implementation of The Contractor’s module components, with the implementation of major changes, and annually thereafter or more frequently as directed by the State. |  |  |  |
| S46 | The Contractor must review any new applicable Contractor provided business processes, including systems and operations under the scope of Subcontractors, for impact on mission critical functionality and update Business Continuity (BC)/Disaster Recovery (DR) and Cyber Incident Response (CIR) Plans prior to new business process implementation that are essential for Vermont to maintain mission critical functionality and key personnel to be contacted at the time of an event. |  |  |  |
| S47 | The Contractor must update key personnel contact information as it relates to the Business Continuity (BC)/Disaster Recovery (DR) and Cyber Incident Response (CIR) Plans immediately upon change. |  |  |  |
| S48 | The Contractor must ensure the Business Continuity (BC)/Disaster Recovery (DR) and Cyber Incident Response (CIR) Plans:a) provide a framework for reconstructing vital operations to ensure the safety of employeesb) provide for the resumption of time sensitive operations and services in the event of an emergencyc) provide for initial and ongoing notification proceduresd) comply with the current version of NIST 800-61 |  |  |  |
| S49 | The Contractor must ensure the Business Continuity (BC)/Disaster Recovery (DR) and Cyber Incident Response (CIR) Plans operational and system functions, including systems and operations under the scope of Subcontractors, must adhere to NIST. These functions may not and cannot be performed and/or stored outside of the United States. |  |  |  |
| S50 | The Contractor must provide an up to date copy of the Business Continuity (BC)/Disaster Recovery (DR) and Cyber Incident Response (CIR) Plans in a secure, highly accessible, centralized online location and at an offsite location approved by the State. |  |  |  |
| S51 | The Contractor must implement a State-approved alert process to handle system related issues, including notifying State identified contacts in accordance with the Business Continuity (BC)/Disaster Recovery (DR) and Cyber Incident Response (CIR) Plans. |  |  |  |
| S52 | The Contractor must provide for backup capabilities at a geographically separate remote site(s) from The Contractor's primary site(s) in accordance with the standards set forth in the Business Continuity (BC)/Disaster Recovery (DR) and Cyber Incident Response (CIR) Plans. System and data back-up and recovery points must be mutually agreed upon between the Contractor and the State. |  |  |  |
| S53 | The Contractor must provide a back‑up and recovery/failover system(s) in compliance with State and Federal rules and regulations to ensure full back‑up. |  |  |  |
| S54 | The Contractor must support an enterprise wide, evolving approach to disaster recovery and continuity of operations needs as the Vermont Medicaid Enterprise transforms. The solution must allow for various types of backups (as designated and approved by the State), in accordance with the approved Business Continuity (BC)/Disaster Recovery (DR) Plan and the criticality and necessity of systems, to eliminate data loss and minimize disruptions to Stakeholders. |  |  |  |
| S55 | The Contractor must ensure that personnel who are responsible for systems recovery and cyber incident response are trained in accordance with NIST Publication 800-53 current revision and tested in their ability to execute the contingency and incident response procedures to which they are assigned. |  |  |  |
| S56 | 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. |  |  |  |
| S57 | Servers will have operating systems hardened by eliminating unnecessary system services, accounts, network services, limited user access rights throughout the environments. |  |  |  |
| S58 | Data Masking is designed to obscure specific data elements and will be used in non-production databases, by replacing actual, regulated data with false, simulated data. |  |  |  |
| S59 | Contractor will log security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to the Environment or Hosting Service Provider Programs, as well as system alerts, console messages, and system errors. The Contractor implements controls to protect against operational problems, including log file media becoming exhausted, failing to record events, and/or logs being overwritten. Security-related log entries will capture the following information: date, time, time zone, user account name and/or IP address, original value, location of change (hostname, filename, table name), new value (other than password). |  |  |  |
| S60 | Self-registered users of applications will have identities verified per NIST SP 800-63-3 |  |  |  |
| S61 | Contractor 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 and document in writing that they have been met. |  |  |  |
| S62 | Deployment environments will be configured with the same security and compliance standards whether production or non-production. |  |  |  |
| S63 | Information assets will have an owner who is responsible for the protection and inventory of assets based on the sensitivity and value of information. If ownership has not been assigned, it will default to the administrators of the application or system. This includes maintenance and operations guides and other documents describing the environments. |  |  |  |
| S64 | Solutions will use Single Sign On (SSO) components for authentication and authorization. |  |  |  |
| S65 | Compliance with FNS Handbook 901 System Security Requirements |  |  |  |
|  |  |  |  |  |

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

**4.4 FNS Compliance Requirements**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID #** | **Non-Functional Requirement Description** | **Comply**  | **Vendor’s Description** **of Applicable Compliance Processes**  | **Audit/Monitor Process** |
| FNS1 | Compliance with FNS Handbook 901 applicable Requirements  |  |  |  |
| 2 | Compliance with Title 7 CFR Parts 271 through 283 |  |  |  |

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

**4.5 Testing Requirements**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID #** | **Non-Functional Requirement Description** | **Comply**  | **Vendor’s Description** **of Applicable Test Management Processes**  | **Audit/Monitor Process** |
| T 1 | Compliance with ISO/IEC/IEEE 29119:1 Standards |  |  |  |
| T 2 | Compliance with ISO/IEC/IEEE 29119:2 Standards  |  |  |  |
| T 3 | Compliance with ISO/IEC/IEEE 29119:3 Standards |  |  |  |
| T 4 | Compliance with FNS Handbook 901 Test Planning Requirements |  |  |  |
| T5 | Compliance with CMS Testing Guidance Framework Requirements  |  |  |  |
| T6 | Compliance with IEEE 1012-2016 |  |  |  |

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

**4.6 Other Non-Functional Requirements**

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

|  |  |  |  |
| --- | --- | --- | --- |
| **ID #** | **Non-Functional Requirement Description** | **Comply** | **Vendor’s Description of Compliance**  |
| O1 | Offer a variable (consumptive) pricing model schedule that allow the State to reduce costs when it can reduce the mainframe resources it consumes (e.g., MIPS consumed, storage consumed, etc..). In vendor’s description of compliance describe what the pricing schedule might look like include any options that the State can consider.  |  |  |
| O2 | Provides customer portal for easy access to reports, billing and support ticketing |  |  |
| O3 | Free use of wireless while in the building for laptops or mobile devices etc. |  |  |
| O4 | Free use of workspace/conference room when working on-site |  |  |
| O5 | Free use of secured shipping/receiving services to hold equipment when it is arriving or leaving. Support of large truck and 18 wheelers for palletized equipment |  |  |
| O6 | Solution implementation must be completed and approved by the State and its Federal partners (e.g., IRS) by 12/31/24. |  |  |
| O7 | Support the State with all required audits (e.g., CMS, FNS, IRS, SSA, etc..) of our operations and execution environments including the support of onsite data center inspections, answering auditor questions, demonstrating operations or application functionality either on site or remotely, and working to remediate any audit findings. |  |  |
|  |  |  |  |

**4.7 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) current revision, Security and Privacy Controls for Information Systems and Organizations
* [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
 |  |  |
|  ☒ 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)
 |  |  |
| ☒Federal Tax Information (FTI) | * Internal Revenue Service Tax Information Security Guidelines for Federal, State and Local Agencies [IRS Pub 1075](https://www.irs.gov/privacy-disclosure/safeguards-program)
 |  |  |
| ☒ Social Security Administration (SSA) | * Social Security Administration (SSA) Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information With the Social Security Administration https://www.ssa.gov/dataexchange/security.html
 |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Type of Data** | **Applicable State & Federal****Standards, Policies, and Laws** | **Comply** | **Vendor’s Description****of Compliance** |
|  ☐Affordable Care Act  Personally Identifiable  Information (PII) | * 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 time-line. 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 considering the content in Appendix 4. 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. 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** | **Vendor Response** |
| System Availability | * The acceptable amount of availability per month is 99.90% for the production environments during business hours and 99.00% outside business hours.
* The acceptable availability per month for non-production environments are 99.90% during business hours and 99.00% outside business hours.
 |  |
| Disaster Recovery: Recovery Time Objective (RTO) and Recovery Point Objective (RPO) | Production environments:* RTO = 2 hours
* RPO = 30 Minutes

All non-production environments:* RTO = 48 hours
* RPO = 48 hours
 |  |
| Plan of Action and Milestones (POA&M) Remediation Service Level Agreement | Contractor will provide a POA&M to the State each quarter which will document the state of current open remediation tasks and historic closed remediations for a period of up to 15 months. Remediate the severity of risk as follows unless as otherwise agreed to by both parties:* Critical ranked risks – shall not exceed more than 15 days in Remediation Status (period of time from the end of the Commencement Phase to Remediation Date).
* High ranked risks – shall not exceed more than 30 days in Remediation Status (period of time from the end of the Commencement Phase to Remediation Date).
* Moderate ranked risks – shall not exceed more than 90 days in Remediation Status (period of time from the end of the Commencement Phase to Remediation Date).
* Low ranked risk – shall not exceed more than 365 days in Remediation Status (period of time from the end of the Commencement Phase to Remediation Date).
 |  |
| 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 | * Contractor 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 Debrief document must be uploaded to “knowledge repository” within five business days of incident closure.
* Root Cause Analysis status must be uploaded to the “knowledge repository” within twenty (20) business days of incident closure.
 |  |
| Helpdesk Response Success Rate | * At least a 90% success rate in completion of service requests for: RACF ID, Adding Disk space, Request for log outputs, T-MON output, Event Data Captures, and ad hoc Reports (as defined by business)
 |  |

\* “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 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.**
2. 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**

1. Submit pricing for your proposed solution in the table below. Fill in only the lines that are applicable to your proposal. **Insert lines for additional costs, but do not delete or rename any lines in the Table**. **Total each column and provide a total of all columns in the “Total Implementation, plus 5 Year Costs” box on the next page.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Cost Type** | **One Time (Implementation)** | **Year 1** | **Year 2** | **Year 3** | **Year 4** | **Year 5** |
| **Hosting** |   |  |  |  |  |  |
| AHS/AOT Hosting \* | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| VDOL Hosting \*  | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| **Implementation Services** |  |  |  |  |  |  |
| Project Management | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| Requirements  | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| Design (Architect Solution) | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| Development (Build, Configure or Aggregate)/Testing | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| System Testing | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| Defect Removal | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| Implement/Deploy | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| Interfaces | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| Quality Management | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| **Cost Type** | **One Time (Implementation)** | **Year 1** | **Year 2** | **Year 3** | **Year 4** | **Year 5** |
| **Implementation Services Continued** |  |  |  |  |  |  |
| Training  | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| Documentation | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
|  | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| **Total Base Costs** | **$0.00** | **$0.00** | **$0.00** | **$0.00** | **$0.00** | **$0.00** |

\*Hosting costs should include all hardware (e.g., CPU, DASD, Tape Solution, VMs, networking gear), software (IBM and 3rd Party), ongoing support and maintenance (including service delivery project management), and the cost of providing a disaster recovery solution. Please note any exceptions from what the State desires to be included in “hosting costs”.

|  |  |
| --- | --- |
| **Total Implementation plus Five Year Costs** | **$ 0.00** |

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. Submit pricing for the following required IT Services that the State may request on an ad hoc basis:

|  |  |  |
| --- | --- | --- |
| IT Services | Title of Position | Hourly Rate |
| Business Analysis: Contractor shall evaluate, document, and recommend changes to business processes and the development, implementation and support of process improvements to eliminate redundancy and increase productivity and reduce cost; interview subject matter experts and others to develop requirements for engineered or commercial off the shelf software and systems. | Senior Business Analysis |  |
| Network Engineer: Contractor shall provide consulting services for LAN/WLAN network Services; functional specifications, network design, network management, data conversion, interfaces, integration, network testing/QA, implementation, training, documentation, and maintenance including version control, support, and issue tracking.Following are Requirements and Capabilities for this Service:* Provide ongoing system, network maintenance and troubleshooting;
* Analyze and document complex network requirements;
* Interpret network requirements, design specifications, manage network development and, integrate and test network components;
* Estimate network development costs and schedules;
* Network integration of multiple complex systems;
* Review existing networks and assist in making refinements, performance improvements, and improving current techniques.
 | Senior Network Engineer |  |
| Database Administrator (DBA): Contractor shall provide supplemental DBA services.Following are Requirements and Capabilities for this Service:* Support of database software (varies by mainframe and application, e.g., ADABAS, VSAM)
* Create Complex Query
* Understanding Database Rules
* Create and update Metadata
* Online Transactional (OLATP)
* Online Analytical (OLAP)
* Database Administration
* Data Warehousing
* Master Data Management
* Install, configure, and upgrade Software AG products (ADABAS, NATURAL, CONSTRUCT, PREDICT).
* Perform ADABAS database administrative tasks, diagnosis and tune, and problem resolution with ADABAS and NATURAL.
* Implement maintenance and fixes to support z/OS upgrades.
 | Senior DBA |  |
| Application Developer: Contractor shall provide supplemental mainframe application development services.Following are Requirements and Capabilities for this Service: Backend and Frontend Developer Services Contractor shall provide services in accordance with the following requirements and capabilities:Primarily responsible for:~~•~~ Application development using VDOL technologies (e.g., Virtual Service Environment (VSE), Computer Programming Language (COBOL), Online System Transaction Processor (CICS), Job Control Language (JCL) and Virtual Storage Access Method (VSAM), Elixir Form Design), includes being mindful of performance constraints around memory, networking availability, etc.• Authoring developer-friendly documentation (e.g., technical design, deployment operations)• Test-driven development• Use of source code version control systems• Relational and non-relational database systems• Handling large data sets and scaling their handling and storage• Communicating technical concepts to a non-technical audience.• Ensuring Section 508 Compliance | Senior VDOL Application Developer |  |
| See senior level description. A non-senior position would have less than 10 years of applicable experience.  | VDOL Application Developer |  |
| Contractor shall provide services in accordance with the following requirements and capabilities:Primarily responsible for:• Application development using AHS technologies (e.g., IBM’s z/OS, Online System Transaction Processor (CICS), Job Control Language (JCL), and Software AG products such as, Adabas, EntireX, Natural Programming Language, Event Replicator, PREDICT, CONSTRUCT and Computer Programming Language (COBOL)), includes being mindful of performance constraints around memory, networking availability, etc.• Authoring developer-friendly documentation (e.g., technical design, deployment operations)• Test-driven development• Use of source code version control systems• Quickly researching and learning new programming tools and techniques• Relational and non-relational database systems• Handling large data sets and scaling their handling and storage• Communicating technical concepts to a non-technical audience.• Ensuring Section 508 Compliance | Senior AHS\AOT Application Developer |  |
| See senior level description. A non-senior position would have less than 10 years of applicable experience.  | AHS\AOT Application Developer |  |

**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:

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

2. 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:

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

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

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

1. **Executive Order 02 – 22: Solidarity with the Ukrainian People**
* By checking this box, Bidder certifies that none of the goods, products, or materials offered in response to this solicitation are Russian-sourced goods or produced by Russian entities. If Bidder is unable to check the box, it shall indicate in the table below which of the applicable offerings are Russian-sourced goods and/or which are produced by Russian entities. An additional column is provided for any note or comment that you may have.

|  |  |
| --- | --- |
| **Provided** **Equipment or Product** | **Note or Comment** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**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:** |  |