**Exhibit C**

moonoververmont

**State of Vermont Bidder Response Form**

**Request for Proposal Name:** *Network Modernization*

**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](mailto:SOV.ThePathForward@vermont.gov)**

## **Part 1: VENDOR PROFILE**

Information directly responding to Items 4 and 5 of Part 1: Vendor Profile may contain confidential information, which must be marked as confidential on the documents. Bidders must also include a copy of documents with the confidential information redacted.

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. Please provide brief summary of your company's history, core competencies, and examples of SD-WAN solutions you have implemented.
     2. Detail your Infrastructure as a Service offerings, specifically how your solutions can support scalable network hardware needs and ongoing management for our state network operations.

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**. . This financial statement or report should demonstrate your company's stability and long-term viability.

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**

Information directly responding to items in Part 2: Vendor Proposal/Solution, Section 3- Security may contain confidential information, which must be marked as confidential on the documents. Bidders must also include a copy of documents with the confidential information redacted.

1. Provide a description of the technology solution you are proposing.
2. Provide a description of the capabilities of the technology solution you are proposing to include answering and/or providing proposed solution details related to each of the following:

|  |  |  |  |
| --- | --- | --- | --- |
| **ID #** | **Vendor’s Proposed Solution** | **Availability** | **Vendor Comments** |
| **1 Architecture** | | | |
| 1.1 | Please provide a detailed description of the functional components of your solution, specifically outlining how it facilitates: |  |  |
| 1.2 | Deployment and management of SD-WAN across branch offices, data centers, and various cloud environments. |  |  |
| 1.3 | Provision of secure and controlled Internet connectivity at branch locations. |  |  |
| 1.4 | Access optimization for cloud services, including both Software as a Service (SaaS) and Infrastructure as a Service (IaaS). |  |  |
| 1.5 | Connectivity solutions for mobile users to seamlessly access resources in physical data centers and cloud-based applications. |  |  |
| 1.6 | Assurance of consistent and reliable global network connections for remote sites, mobile users, and cloud platforms. |  |  |
| 1.7 | Describe how your solution integrates network functions SD-WAN, its scalability for adding capacity and sites, and its approach to ensuring high availability and resiliency. |  |  |
| 1.8 | Provide information on your solution's management and reporting tools, detailing the process for software updates, including automation and customization options. |  |  |
| 1.9 | Explain how your architecture supports state government needs in terms of simplifying network management, improving agility, and bolstering security. |  |  |
| 1.10 | Include a diagram illustrating the solution's implementation in a state government network context. |  |  |
| **2 SD-WAN** | | | |
| 2.1 | WAN Connectivity Management: |  |  |
| 2.1.1 | Describe the ability of your solution to support and manage a range of WAN links (Ethernet, xDSL, GPON, Fiber, 4G/LTE, etc.) in a multi-homed environment. |  |  |
| 2.1.2 | Link Aggregation Resilience: Explain how Active/Active and Active/Passive link aggregation are managed in your solution, especially in maintaining continuous connectivity during disruptions like a fiber cut. |  |  |
| 2.1.3 | Detail your solution's methods for detecting link degradation and complete outages, and the metrics used for such assessments. |  |  |
| 2.1.4 | Outline the automated failover and recovery actions your solution implements to address link failures and degradation, with a particular focus on restoring VPN tunnels promptly in multi-homed environments. |  |  |
| 2.2 | Traffic Routing and Quality of Service: |  |  |
| 2.2.1 | Please specify what types of identifiers (such as IPv4/IPv6 addresses , hostnames, applications, user or group IDs) your system can utilize for defining traffic routing policies. Also, can custom rules be established for proprietary or specialized applications within our network? |  |  |
| 2.2.2 | Indicate the number of applications your system recognizes by default for traffic management. Describe the process and levels of granularity available for prioritizing traffic, including how different applications, user groups, or data types can be assigned priority. |  |  |
| 2.2.3 | Explain your system's approach to ensuring that high-priority or critical applications always receive the necessary bandwidth, particularly during network congestion or peak usage times. |  |  |
| 2.3 | Voice and Latency-Sensitive Traffic Management: |  |  |
| 2.3.1 | Describe how your Quality of Service (QoS) mechanisms are designed to support voice applications and other latency-sensitive traffic, including their effectiveness in environments with NAT traversal. |  |  |
| 2.3.2 | Detail the specific features and capabilities your system provides to support and enhance the quality of voice communications, especially in scenarios involving NAT traversal. |  |  |
| 2.3.3 | Voice Call Continuity during Link Degradation: Explain the strategies or technologies your system employs to maintain the continuity and quality of voice calls, particularly in the event of network link degradation, and how these strategies handle NAT traversal challenges. |  |  |
| 2.4 | Throughput and Edge Device Capabilities: |  |  |
| 2.4.1 | Outline the range of throughputs your solution supports and describe your methodology for sizing the solution to meet specific throughput requirements. |  |  |
| 2.4.2 | Explain the different types of devices and models your solution offers to deliver the supported throughput levels. Please include how these devices vary in terms of performance capabilities. |  |  |
| 2.4.3 | Provide any documentation or guidelines used for determining the actual throughput capabilities based on various customer requirements, such as network size, traffic decryption, routing complexity, and security inspection processes. |  |  |
| 2.5 | Monitoring and Reporting Capabilities: |  |  |
| 2.5.1 | Specify the range of network entities your solution monitors, including locations, links, applications, users, and hosts. |  |  |
| 2.5.2 | Metrics and Data Views: Describe the metrics tracked for each monitored entity and indicate whether your system provides both real-time and historical data views. |  |  |
| 2.5.3 | Detail your approach for investigating network incidents to identify the root cause. |  |  |
| 2.5.4 | Provide screenshots or visual examples demonstrating how your solution visualizes the entire network, individual sites, multiple links, and specific hosts, showcasing both historical and real-time data perspectives. |  |  |
| 2.6 | Site Provisioning and Gradual Deployment with Diverse Connectivity: |  |  |
| 2.6.1 | Describe the procedure for adding a new site to your SD-WAN solution, considering various connectivity types. |  |  |
| 2.6.2 | Explain the process for setting up high availability at a site with dual edge devices within your SD-WAN system. |  |  |
| 2.6.3 | Provide a strategy for the gradual implementation of your SD-WAN solution, emphasizing its compatibility and integration with a range of existing network infrastructures. |  |  |
| 2.6.4 | Explain how your SD-WAN solution coexists and interacts with a variety of network types at a single location, including support for sites connected via these networks but not directly on your SD-WAN. |  |  |
| **3 Security** | | | |
| 3.1 | SD-WAN Security – Encryption and Threat Management: |  |  |
| 3.1.1 | Describe your approach to providing end-to-end encryption within the SD-WAN and discuss any impact this encryption has on network throughput. |  |  |
| 3.1.2 | Outline your solution's threat prevention capabilities, including URL filtering, various types of malware protection (signature and non-signature based), and IPS. Also, describe the configuration, customization of policies, and the integration method for these features, whether built-in or through service chaining. |  |  |
| 3.1.3 | Explain how your solution performs deep packet inspection to identify and mitigate threats, particularly in scenarios where all traffic is encrypted, and assess the impact on overall SD-WAN throughput in such cases. |  |  |
| 3.2 | Branch Security in SD-WAN: |  |  |
| 3.2.1 | Detail the specific security services your solution offers for direct Internet traffic at branch locations, including capabilities like URL Filtering, Anti-malware, and Intrusion Prevention Systems (IPS). |  |  |
| 3.2.2 | Clarify what types of physical or virtual appliances are necessary for implementing these security services at branch sites. Also, specify any cloud-based services that need to be acquired to fully secure branch Internet traffic. |  |  |
| 3.2.3 | Describe the management process of your branch security solution, emphasizing whether it is seamlessly integrated with the SD-WAN management system, and how this integration enhances operational efficiency. |  |  |
| 3.2.4 | Provide a comprehensive overview of your threat prevention and detection strategies for branch traffic, detailing how these measures are tailored to address the unique security challenges at branch locations. |  |  |
| 3.3 | Cloud and Mobile Security in SD-WAN: |  |  |
| 3.3.1 | Explain your strategies for securing traffic to and from cloud datacenters, public cloud applications, and between mobile users and cloud/on-premises applications. Highlight any specific technologies or methodologies employed. |  |  |
| 3.3.2 | Detail the required components, both hardware and software, for ensuring security in cloud access and mobile user scenarios. |  |  |
| 3.3.3 | Describe how both cloud and mobile security solutions are managed within your SD-WAN framework. Emphasize the integration of these security solutions with the SD-WAN management platform and the operational benefits of this integration. |  |  |
| 3.4 | Identity, Policy Management, and Security Analytics in SD-WAN: |  |  |
| 3.4.1 | Discuss how user and group identities are linked to network flows and incorporated into network and security policies. Include details on maintaining synchronization with federated identity management systems like Azure AD. |  |  |
| 3.4.2 | Describe how security policies are enforced across various levels (branch, user group, entire network) and detail the default policies available out of the box. Explain how these can be customized. |  |  |
| 3.4.3 | Describe access control mechanisms for the security management console and detail the types of security events generated. Highlight the default security capabilities, their customization options, and the analytics and reporting features available for monitoring and managing these events. |  |  |
| **4 Cloud** | | | |
| 4.1 | Cloud Integration and Traffic Optimization in SD-WAN: |  |  |
| 4.2 | Elaborate on the specific components and detailed procedures required to connect a cloud datacenter, such as AWS or Azure, into your SD-WAN. Include information on any specialized hardware or software, network configurations, and security protocols needed. |  |  |
| 4.3 | Clarify if the cost for integrating both cloud datacenters (like AWS and Azure) and cloud-based applications is covered within the quoted price and specify any conditions or additional charges that may apply. |  |  |
| 4.4 | Specify your solution's compatibility and integration capabilities with major cloud datacenter providers, particularly focusing on AWS and Azure. Discuss any existing partnerships or optimized pathways that facilitate seamless integration with these platforms. |  |  |
| 4.5 | Detail the specific technologies or methodologies your solution employs to optimize network traffic from various locations and mobile users to cloud datacenters, emphasizing how these strategies are adapted for AWS and Azure environments. |  |  |
| 4.6 | Describe how your solution enhances traffic flow and performance to various cloud applications, including cloud storage, CRM, ERP, and Office 365, especially when these applications are hosted on AWS or Azure. Highlight any unique features or algorithms used to ensure efficient and secure access to these cloud services. |  |  |
| **5 Mobile** | | | |
| 5.1 | Mobile Connectivity and Optimization in SD-WAN: |  |  |
| 5.2 | Thoroughly describe how your solution connects mobile users to the SD-WAN. Include specifics about any protocols, authentication mechanisms, and configurations used, particularly how these integrate with cloud environments like AWS and Azure. |  |  |
| 5.3 | Detail the various methods available for mobile users to access the WAN and cloud services, including VPN clients and clientless solutions. Explain how these options are optimized for accessing resources on cloud platforms such as AWS and Azure. |  |  |
| 5.4 | Describe the optimization techniques your solution uses for mobile traffic directed towards different applications, whether in physical datacenters, cloud datacenters like AWS and Azure, or public cloud applications including Office 365. Highlight how these methods improve performance and security. |  |  |
| 5.5 | Describe the unique benefits and features of your solution for mobile connectivity compared to legacy VPNs and zero trust solutions, with a focus on enhanced compatibility and performance with cloud services from AWS and Azure. Emphasize improvements in security, user experience, and scalability that are particularly relevant for cloud-centric environments. |  |  |
| **6 Global** | | | |
| 6.1 | Explain how your SD-WAN solution optimizes traffic between Vermont's local data centers and major cloud platforms like Azure and AWS. Include strategies for ensuring efficient data flow and minimizing latency. |  |  |
| 6.2 | Detail the Service Level Agreements (SLAs) your solution provides, focusing on latency, packet loss, and jitter, particularly in the context of traffic between Vermont and cloud services in Azure and AWS. |  |  |
| 6.3 | Third-Party Components for Optimal Performance: Specify any third-party components required to optimize traffic performance both globally and specifically with cloud platforms such as Azure and AWS. |  |  |
| 6.4 | Describe how your SD-WAN solution ensures an optimal network experience for mobile users, particularly those accessing Vermont's local data centers and cloud resources in Azure and AWS. |  |  |
| **7 Support & Professional Services** | | | |
| 7.1 | Cost and Resource Efficiency: Optimizes network operations to minimize both operational and capital expenses. |  |  |
| 7.2 | Transparent Licensing: Provides clear and predictable licensing models. |  |  |
| **8 Managed Services** | | | |
| 8.1 | Describe if your company offers follow-the-sun support, ensuring consistent and uninterrupted assistance across different time zones. Provide details on how this model facilitates timely support responses regardless of geographic location. |  |  |
| 8.2 | Specify the exact geographic locations of your support centers. Detail how these locations contribute to the efficiency and effectiveness of your support, particularly in terms of language capabilities, regional knowledge, and time zone coverage. |  |  |
| 8.3 | Confirm the availability of your support services on a 24/7/365 basis. Elaborate on how your support structure is organized to handle off-hours, weekends, and holiday support inquiries, ensuring continuous operational support. |  |  |
| 8.4 | Provide a comprehensive breakdown of your support Service Level Agreements. This should include information on the different tiers of support offered (if applicable), average response and resolution times, and escalation procedures for critical issues. |  |  |
| 8.5 | Clarify whether professional services are provided in-house by your organization or through certified partners. Detail the range of services offered in areas like network planning, system design, deployment strategies, implementation processes, and training programs. Also, highlight the qualifications and experience levels of the personnel involved in delivering these services, whether they are in-house experts or partner-affiliated professionals. |  |  |
| **9 Managed Services** | | | |
| 9.1 | Provide a detailed description of your managed services, covering areas such as last-mile monitoring, Managed Detection and Response (MDR), and comprehensive management of networking and security policies. |  |  |
| 9.2 | Explain whether managed services are available both as a complete package and on an a-la-carte basis. Detail the different levels of service management available, from self-service to fully managed, and describe the scope of control and support offered at each level. |  |  |
| 9.3 | Discuss any restrictions on self-service modifications under a managed service agreement and the extent of visibility and control provided in fully managed services, with a focus on network and security monitoring. |  |  |
| 9.4 | Describe your Uninterrupted Power Supply (UPS) systems, including their types, capacity, and integration into network infrastructure for ensuring power continuity during outages. |  |  |
| 9.5 | Elaborate on your Infrastructure as a Service (IaaS) offerings. Detail the availability of on-demand enterprise-grade network hardware and software, the full scope of lifecycle management provided. |  |  |

1. 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:
2. 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).
3. List the total number of installations in the last 3 years by the year of installation.
4. Provide the total number of current users for the proposed system and indicate what version they are using.
5. Have you implemented the proposed solution for other government entities? If so, tell us who, when, and how that implementation went?
6. **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.**
7. **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.**
8. Does your proposed solution include any warranties? If so, describe them and provide the warranty periods.
9. Describe any infrastructure, equipment, network or hardware *required* to implement and/or run the solution.
10. What is your recommended way to host this solution?
11. Describe how your solution can be integrated to other applications and if you offer a standard-based interface to enable integrations.
12. 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**

Information directly responding to items in Part 3: Functional Requirements, Section 3- Security may contain confidential information, which must be marked as confidential on the documents. Bidders must also include a copy of documents with the confidential information redacted.

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 Architecture** | | | |
| 1.1 | Application-Centric Network Management: Optimizes the network for critical applications to enhance performance and user experience. |  |  |
| 1.2 | Transport-Independent Fabric: Provides flexibility to work over various transport technologies, ensuring reliable connectivity. |  |  |
| 1.3 | Scalable Network Infrastructure: Adapts to changing business needs and scales efficiently. |  |  |
| 1.4 | Model-Driven Templates: Simplifies network configurations and speeds up deployment. |  |  |
| 1.5 | Secure and Resilient Connectivity: Offers robust and secure connectivity, essential for cloud-centric and distributed environments. |  |  |
| 1.6 | IPv6 Readiness: Future-proofs the network by ensuring compatibility with IPv6. |  |  |
| 1.7 | RESTful API Integration: Features comprehensive RESTful APIs, enabling custom automation and seamless integration into diverse workflows, essential for network management and development flexibility. |  |  |
| **2 SD-WAN** | | | |
| 2.1 | DevOps Integration: Supports agile network changes, enhancing the network's ability to support business demands. |  |  |
| 2.2 | Advanced Access Control and Segmentation: Enhances security and management with sophisticated access control. |  |  |
| 2.3 | Intent-Based Networking Capabilities: Utilizes business intent for network configurations, streamlining management. |  |  |
| 2.4 | Enhanced Network Assurance: Improves network security and simplifies identity management. |  |  |
| 2.5 | Automated Policy Enforcement: Streamlines management with automated policy applications. |  |  |
| 2.6 | AI-Driven Insights and Automation: Uses AI to analyze network data for predictive management and automated optimization. |  |  |
| 2.7 | Intelligent Path Selection: Dynamically selects the best network path based on real-time conditions for optimal performance. |  |  |
| 2.8 | Streamlined Network Operations: Automates network tasks for increased efficiency and reduced manual intervention. |  |  |
| **3 Security** | | | |
| 3.1 | Robust Security Posture: Incorporates comprehensive security measures for network protection. |  |  |
| 3.2 | Zero Trust Security Framework: Adopts a stringent security model, not inherently trusting any network entity. |  |  |
| 3.3 | End-to-End Network Segmentation: Improves security by segmenting the network to contain threats. |  |  |
| 3.3 | Compliance with Standards: Meets regulatory compliance requirements and adheres to industry security standards. |  |  |
| 3.4 | Specific Security Standards: Vendors must demonstrate and maintain compliance with specific security standards relevant to our operations, such as the Criminal Justice Information Services (CJIS) and IRS Publication 1075. |  |  |
| 3.5 | Comprehensive Threat Detection: Provides real-time monitoring and detection of DDoS threats to ensure network availability. |  |  |
| 3.6 | Adaptive Threat Mitigation: Dynamically adjusts security measures to counteract evolving DDoS attacks. |  |  |
| 3.7 | Resilient Infrastructure Protection: Strengthens network defenses to withstand and repel volumetric DDoS attacks. |  |  |
| 3.8 | Intelligent Traffic Analysis: Employs advanced analytics to differentiate between legitimate traffic and DDoS, and other threats. |  |  |
| 3.9 | Automated Attack Response: Initiates immediate, automated responses to detected DDoS and other incidents to minimize downtime. |  |  |
| **4 Cloud** | | | |
| 4.1 | Cloud-Native Management Platform: Centralizes management in the cloud for scalability and easy integration with cloud services. |  |  |
| 4.2 | Reliable Application Performance: Ensures consistent application performance, critical for maintaining service levels. |  |  |
| **5 Mobile** | | | |
| 5.1 | Organizational Adaptability: Assists in adapting to evolving network technologies and methodologies. |  |  |
| **6 Global** | | | |
| 6.1 | Global Network Support: Ensures consistent service quality across geographically diverse locations. |  |  |
| **7 Support & Professional Services** | | | |
| 7.1 | Cost and Resource Efficiency: Optimizes network operations to minimize both operational and capital expenses. |  |  |
| 7.2 | Transparent Licensing: Provides clear and predictable licensing models. |  |  |
| **8 Managed Services** | | | |
| 8.1 | Reliable Power Backup: Ensures uninterrupted power supply (UPS) for critical systems during power outages. |  |  |
| 8.1.1 | Uninterrupted Power Solutions Compliant with NFPA 855: Fully compliant with NFPA 855 standards for safety and performance in stationary energy storage systems. |  |  |
| 8.2 | IaaS Network Provisioning: Provides enterprise-grade network hardware and software on-demand, coupled with full lifecycle management, to meet dynamic business requirements and ensure uninterrupted service delivery. |  |  |

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

Information directly responding to items in Part 4: Non-Functional Requirements, Section 4.3- Security may contain confidential information, which must be marked as confidential on the documents. Bidders must also include a copy of documents with the confidential information redacted.

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. |  |  |

**4.2 Application Solution**

|  |  |  |  |
| --- | --- | --- | --- |
| A1 | Any solutions vendor must provide for the backup/recover, data retention and disaster recovery of a contracted/hosted application solution. |  |  |
| A2 | Any solutions vendor must provide for application management and design standard of all technology platforms and environments for the application solution (Development, Staging, Productions, DR, etc.) |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID #** | **Non-Functional Requirement Description** | **Comply** | **Vendor’s Description of Compliance** |
| A3 | Any solutions vendor must engage the State of Vermont using Service Level Agreements for system and application performance, incident reporting and maintenance. |  |  |
| A4 | 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. |  |  |
| A5 | As a contract deliverable, the vendor shall supply an up-to-date data dictionary that represents all data respective of the solution it will provide.  The data dictionary must contain the following attributes:   1. The technology (RDBMS platform) that hosts the data source, i.e. Oracle, SQL Server, MySQL, DB2, etc. 2. The location where the data source is hosted 3. Thorough descriptions of each table in the data source 4. Thorough descriptions of each column within each table in the data source.  In addition to business definitions, column descriptions must include the following detail: schema names; file group names (if applicable); data types; lengths; primary and foreign key constrains; applied formatting; applied calculations; applied aggregations; NULL-ability; default values. |  |  |

**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 | Input validation |  |  |  |
| S2 | Output encoding |  |  |  |
| S3 | Authentication and password management |  |  |  |
| S4 | Session management |  |  |  |
| S5 | Access control |  |  |  |
| S6 | Cryptographic practices |  |  |  |
| S7 | Error handling and logging |  |  |  |
| S8 | Data protection from unauthorized use, modification, disclosure or destruction (accidental or intentional). |  |  |  |
| S9 | Communication security |  |  |  |
| S10 | System configuration |  |  |  |
| S11 | Database security |  |  |  |
| S12 | File management |  |  |  |
| S13 | Memory management |  |  |  |
| S14 | Fraud detection |  |  |  |
| S15 | General coding practices |  |  |  |
| S16 | POA&M management |  |  |  |
| S17 | Risk Assessment Practices including but not limited to vulnerability assessment and pen testing |  |  |  |
| S18 | Incident response planning and testing |  |  |  |
| S19 | System Security Plan delivery |  |  |  |
| S20 | Solutions service provider is responsible for authorizing its personnel to access all environments through network and system authorization processes. |  |  |  |
| S21 | The network will ensure a secure environment by employing redundant firewalls, intrusion detection systems (IDS), syslog, and VPN technologies. The firewall security policy will strictly enforce default-deny rule sets, and an IDS will actively monitor for any potential breaches of predefined rules. |  |  |  |
| S22 | The solutions service provider will implement Internet Protocol Security (IPsec) as part of an overall VPN strategy to secure data between endpoints on the management link by employing tunneling and encryption to facilitate data privacy. |  |  |  |
| S23 | The solutions service provider is tasked with defining, designing, and implementing a network transport system. This system will enable personnel to access their environment, such as Transaction Link. VPN tunnels will connect the DMZ at the SOV data centers, terminating on the hosting service provider firewalls. |  |  |  |
| S24 | Access to logs will be provided on a need-to-know and least privileged basis. Log files will be protected by SHA1 cryptographic hash sum and are monitored. Logs on intranet-accessible systems are relocated daily to systems that are not intranet- accessible. Logs on systems that are accessible within the intranet are relocated daily to systems that are not intranet-accessible. This practice enhances security by isolating the logs from systems that may be vulnerable to intranet-based threats. It also provides a level of separation between the log data and potential attackers who might have gained access to intranet-accessible systems. |  |  |  |
| S25 | The State of Vermont security office will authorize all repairs and modifications to the security barriers or entry controls on the network. |  |  |  |
| S26 | The network service provider will employ network controls to address the protection and control of the State of Vermont (SOV) data during its transmission from one end system to another. All computers, servers, and other data devices connected to the hosting service provider network will comply with the hosting service provider standards for security, configuration, and access method, in accordance with the State of Vermont security policies. |  |  |  |
| S27 | Cryptographic controls will be implemented using IPsec and SSL protocols to provide end users, whether they are the State of Vermont’s (SOV's) end users or the network service provider support engineers, with secure access to the target applications. |  |  |  |
| S28 | VPN tunnel endpoints will be encrypted with (minimally) 168-bit Triple DES. |  |  |  |
| S29 | Network device configurations will be hardened by performing the following: Disabling telnet access. Controlling Simple Network Management Protocol (SNMP) access to devices. Controlling access to devices through the use of Terminal Access Controller Access Control System Plus (TACACS+). Turn off unneeded services. Perform appropriate level of logging. |  |  |  |
| S30 | The HIPAA security services involve implementing specific security controls to safeguard the confidentiality, integrity, and availability of the State of Vermont's (SOV's) electronic Protected Health Information (ePHI) stored within the hosting service provider's data center(s). These services are tailored to assist the SOV in fulfilling its legal responsibilities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its amendments through the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). These regulations apply to the hosting service provider's management of the SOV's hosted environments containing ePHI. Periodic modifications to the HIPAA Security Services will be made through the change management process to align with evolving industry standards or legal obligations, as determined by the hosting service provider. |  |  |  |
| S31 | The network hosting service provider will conduct quarterly reviews of the firewall policies and network devices configurations for the State of Vermont’s (SOV's) hosting service provider ePHI Environments; annually for HIPAA. |  |  |  |
| S32 | Network solutions providers will have critical security patches applied within 24 hours of the patch release. |  |  |  |
| S33 | The network systems must have robust audit trails to track and log all activities related to a communication or transaction to provide evidence in the event of a dispute. |  |  |  |
| S34 | The network solutions provider must support end-to-end encryption for all data traversing the network infrastructure carrying CJIS data. Use strong encryption protocols to safeguard the confidentiality and integrity of the data during transmission, reducing the risk of interception or tampering. |  |  |  |
| S35 | For FERPA (Family Educational Rights and Privacy Act) data, the network solutions provider must implement network segmentation to segregate FERPA data traffic from other non-FERPA data. This helps minimize the risk of unauthorized access and containment in the event of a security breach, ensuring that FERPA data remains protected within dedicated network segments. |  |  |  |
| S36 | For HIPAA ( Health Insurance Portability and Accountability Act) data, the network solutions provider must implement network segmentation to segregate HIPAA data traffic from other non-HIPAA data. This helps minimize the risk of unauthorized access and containment in the event of a security breach, ensuring that HIPAA data remains protected within dedicated network segments. |  |  |  |
| S37 | The network solution provider must ensure ZTP (zero-touch-provisioning) the acceptable time for devices to be provisioned. |  |  |  |
| S38 | The network solution provider must ensure ZTP include error handling such as notifications, logging and automated recovery. |  |  |  |

**4.4 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** | **Availability** | **Vendor Comments** |
| **Analyzability** | | | |
| AN1 | The solution must have clear and detailed documentation, including design and architecture documents, API specifications, and user manuals. |  |  |
| AN2 | The solution must support monitoring and logging of system events and errors to facilitate root cause analysis and troubleshooting. |  |  |
| AN3 | The solution must support automated analysis tools for identifying and reporting on issues such as code quality, security vulnerabilities, and performance bottlenecks. |  |  |
| AN4 | The solution architecture will allow for transaction tracking and review throughout the system for auditing, error diagnosis, and performance management purposes. |  |  |
| AN5 | Solutions Providers will use the State requirements to design the Solutions Provider environments and prepare a provisioning release plan. |  |  |
| AN6 | 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. |  |  |
| AN7 | Solutions will have the capability to track and report usage. |  |  |
| AN7 | 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. |  |  |
| AN8 | Solutions will automatically calculate transfer and destruction dates (and assign records ready for deletion to the appropriate review process for approval of final deletion) for all records in the retention schedules. |  |  |
| Availability | | | |
| AV1 | If necessary, based on the requirements of the solution, the provider will provide a dedicated circuit for the State's Internet circuit that is only used for The solution provider Services. A dedicated circuit will help prevent problems related to overuse by isolating traffic to The solution provider from the State's other Internet traffic. A dedicated circuit will help achieve stable and predictable Network Connectivity. The solution provider will not use the State internet circuit. |  |  |
| AV2 | 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). |  |  |
| AV3 | Solutions will provide the ability to recover from data loss due to end user error and end application error. Recovery includes the following: \* The ability to recover from data loss: 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. \* 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. \* 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. |  |  |
| AV4 | The solution must detect and capture errors; and identify their causes. Failures require notification to the State of Vermont within a period of time specified in the SLA. |  |  |
| AV5 | Solutions will be architected with no single point of failure, supporting a high-availability enterprise. |  |  |
| AV6 | 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. |  |  |
| AV7 | For PaaS and IaaS solution providers, backup and Recovery Services will include operating system images, configuration files, database, code tree, hardware configurations and virtualization configurations. (PaaS, IaaS) |  |  |
| AV8 | Solutions will include a disaster recovery plan and provide contingency plans to the State for application services managed by the solution provider. |  |  |
| AV9 | If determined that deployment at the Disaster Recovery (DR) site is required for restoration and use of the Production Environment, the solution provider will use reasonable efforts to provide the State with information for DR cutover. |  |  |
| AV10 | 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. |  |  |
| AV11 | 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. . |  |  |
| AV12 | 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. |  |  |
| AV13 | 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. |  |  |
| AV14 | The solution provider will report Outages and Service Interruptions when identified per the SLA. |  |  |
| AV15 | Solution provider will monitor critical performance parameters: these can include:  \* CPU usage: the percentage of CPU resources consumed by the software. High CPU usage can affect the responsiveness and speed of the solution. \* Memory usage: the amount of memory allocated by the software. High memory usage can indicate high resource consumption and affect the performance of the solution \* Requests per minute and bytes per request: the number of requests received by the software’s API per minute and the amount of data handled by each request.  \* Latency and uptime: the delay between a user’s action on the software and the response of the software to that action, and the availability of the software to serve requests.  \* Security exposure: the degree to which the software is vulnerable to unauthorized access, modification, or damage.  \* Execution time: the time taken by the software to complete a certain function or task.  \* Throughput: the rate at which the software can process data or transactions. |  |  |
| AV16 | The solutions provider will send alarms based on the monitored attributes. These will be escalated through eMail and SMS. |  |  |
| AV17 | 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. |  |  |
| AV18 | The solution provider will schedule routine planned maintenance activities without disrupting the operational hours. |  |  |
| AV19 | The solution provider will assist the State in identifying root causes for all Solution interface related problems. |  |  |
| AV20 | IaaS The solution provider will comply with Service Level Agreements for the solution. |  |  |
| AV21 | The IaaS solution provider will build the State's infrastructure utilizing physical and virtual separation of components. (IaaS) |  |  |
| AV22 | The IaaS solutions provider will supply environments that are scalable, enterprise-ready applications. These include, sandboxes, testing platforms, staging platforms and development platforms as need for the solution. |  |  |
| AV23 | The IaaS solution provider must support hardware and network load balancing technologies for high availability and maintenance. (IaaS) |  |  |
| Compatibility | | | |
| CO1 | If the solution requires, the service provider will supply VPN devices for installation on the State of Vermont's internal network, or approve the installation of State of Vermont-provided network equipment, provided it complies with the approved SOV network architecture solution. |  |  |
| CO2 | If necessary and required for the solution, Service Provider will provide public Internet addresses for devices that require Internet access, and service provider will provide public addresses for equipment interfaces that connect to the Service Provider network. |  |  |
| CO3 | If necessary and required for the solution, the service provider will use NAT and PAT to map private addresses to public addresses. They will provide and maintain public IP addresses, using one-to-one static NAT for all network devices that the service provider initiates a connection with, including SOV printers or print servers. PAT is allowed for network devices that initiate connections with the service provider, such as user workstations connecting to the service provider programs. |  |  |
| CO4 | If necessary and required for the solution, in order to avoid IP address conflicts, service provider will route network traffic to globally unique public IP addresses registered through one of the regional Internet registry organizations. The service provider will not route traffic to private IP addresses. |  |  |
| CO5 | Solutions will provide the ability for on-line access by any site connected to the State of Vermont's Network. |  |  |
| CO6 | The software shall undergo rigorous compatibility testing with future versions of the software, ensuring that any potential issues are identified and resolved before the release of the new version. This testing should cover all aspects of the software, including hardware, software, and network configurations. |  |  |
| CO7 | The software shall undergo rigorous compatibility testing in different environments and configurations, ensuring that it can operate correctly and perform well under various conditions. This testing should cover a range of hardware, software, and network configurations, and be performed on both new and legacy systems. |  |  |
| Maintainability | | | |
| MANT1 | If required for the solution, the network design and network connection configuration, which includes a detailed cabling diagram for network connections between State and Solutions Provider data center locations, will be the responsibility of the Solutions Provider. |  |  |
| Maturity | | | |
| MAT1 | 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: Perform problem analysis: The solution provider will investigate and identify the root causes of any incidents that affect the availability of the solution. 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. Enhance service quality: The solution provider will aim to improve the value and satisfaction delivered by the solution to the State and its users. 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. |  |  |
| MAT2 | The solution provider will provide the status of Root Cause Analysis for Severity Level 1 Unplanned Outages, as defined in Service Level Agreement. (SaaS) |  |  |
| MAT3 | The solution provider will conduct an implementation readiness review at least ten days prior to production cutover. |  |  |
| MAT4 | The solution provider will be accountable for all end-to-end and integration testing for the applications that they built including all external interfaces. |  |  |
| MAT5 | During testing, the solution provider will identify event-thresholds to be used for benchmarking the performance of the solution. (SaaS) |  |  |
| MAT6 | 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. |  |  |
| MAT7 | The solution provider will prepare User Acceptance Testing (UAT) Plan to include, Unit, Integration, SIT, Regression, Stress/Performance. |  |  |
| MAT8 | The IaaS solution provider will utilize industry standard virtualization technologies, and will deploy said virtualization technologies following the best practices of the selected virtualization the solution provider(s). (IaaS) |  |  |
| Modifiability | | | |
| MO1 | The solution must support the addition of new functionality, modules, and components without requiring extensive modifications to the existing system |  |  |
| MO2 | The solution must support the modification of existing functionality, modules, and components without introducing unintended consequences or side effects. |  |  |
| MO3 | The solution must support version control and rollback capabilities to facilitate quick and easy reversions in case of errors or issues with new updates. |  |  |
| MO4 | To maintain the accuracy and integrity of the data, SaaS and PaaS solution providers must perform regular data system refreshes. |  |  |
| MO5 | Solutions Provider will develop with State approval, a Refresh Schedule to perform the Refreshes identified. |  |  |
| MO6 | Solutions Provider will perform Refreshes based on a submitted and approved change request from the State. |  |  |
| MO7 | 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. |  |  |
| MO8 | Solutions will ensure version control of documents as they are changed or modified. |  |  |
| MO9 | Solutions will have the ability to automate, based on rules or context, the creation of indexing, meta data and overall taxonomy. |  |  |
| Modularity | | | |
| MOD1 | The solution must have clear and well-defined module boundaries to minimize the risk of side effects or unintended consequences. |  |  |
| MOD2 | The solution must support independent deployment of modules, allowing for more frequent updates and reducing the risk of system-wide downtime during maintenance. |  |  |
| MOD3 | The solution must be modular, with components that can be easily added, removed, or replaced. |  |  |
| MOD4 | If required for the solution, the network design and network connection configuration, which includes a detailed cabling diagram for network connections between State and Solutions Provider data center locations, will be the responsibility of the Solutions Provider. |  |  |
| MOD5 | Solutions will be scalable and adaptable to meet future growth and expansion needs such that Solutions will be expanded and be able to retain its performance levels when adding additional users, functions, and data. |  |  |
| MOD6 | 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 enAs part of the Run Book delivered prior to go-live, the Solutions Provider will maintain a logical Architecture Document that outlines the current configuration of all modular components, including third-party applications, in all environments. |  |  |
| MOD7 | With solutions, any changes or updates to the components that are shared across different systems and locations can be managed and applied from one place and take effect immediately. |  |  |
| MOD8 | Solutions will have the ability to find broken links or orphaned documents not associated to another object. |  |  |
| MOD9 | Solutions Provider will install and manage required third party software. |  |  |
| Performance Efficiency | | | |
| PE1 | Hosting service provider will implement minimum bandwidth requirements as a starting point for network sizing deployment. |  |  |
| Recoverability | | | |
| REC1 | Solution providers must test Backup/Recovery procedures prior to the production launch of the system to validate the procedures and affirm ability to meet recovery requirements. |  |  |
| REC2 | The recovery point objective (RPO) will meet State requirements as defined in the Service Level Agreement. |  |  |
| REC3 | The recovery time objective (RTO) will meet State requirements as defined in the Service Level Agreement. |  |  |
| REC4 | The solution provider will comply with the State's Disaster Recovery Plan for the entire solution based on the assumption that Solution's data will be recovered at an alternate data center as designated by the State. |  |  |
| REC5 | The solution provider will provide Service Continuity Management for the Production Environment following a declared Disaster. |  |  |
| REC6 | 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. |  |  |
| Reliability | | | |
| REL1 | The IaaS solution provider must support hardware and network load balancing technologies for high availability and maintenance. (IaaS) |  |  |
| Reusability | | | |
| REU1 | Solutions Provider will assist the State in preparing the detailed infrastructure requirements. |  |  |
| REU2 | When proposing changes to the architecture of the solution, the solution provider will generate an updated logical architecture diagram. |  |  |
| REU3 | Solutions Provider will use DNS instead of host files. |  |  |
| REU4 | Solutions Providers will provide a data dictionary and data model to the State. |  |  |
| REU5 | 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. |  |  |
| REU6 | 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 rules repository. |  |  |
| REU7 | For document management functions, Solutions will use a centralized, shared document management/content management solution. |  |  |
| Scalability | | | |
| SCL1 | The network solution must provider for expectations bandwidth, allowing the network to adapt to increased data transfer requirements without degradation in performance. |  |  |
| SCL2 | The network solution must ensure that the architecture allows for scalable segmentation to support different business units or departments. |  |  |
| SCL3 | The network solution must include features that support capacity planning, helping the State of Vermont proactively manage and allocate resources based on anticipated growth. |  |  |
| SCL4 | The network solution provider must provide information on the scalability-related costs, both in terms of initial investment and ongoing operational expenses. |  |  |
| Testability | | | |
| TST1 | The solution must support automated testing, with clear and well-defined test cases and test data. |  |  |
| TST2 | The solution must have clear and well-defined interfaces and APIs for testing and simulation purposes. |  |  |
| TST3 | The solution must support the use of testing and simulation tools to facilitate unit testing, integration testing, and performance testing. |  |  |
| TST4 | 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. |  |  |
| TST5 | Solutions Providers will conduct testing on any changes to ensure backward compatibility of its Solution and integration within the State's environments. |  |  |
| TST6 | Solutions will have the ability to generate administrative alerts and warnings when statistics indicate an impact or potential limits on solution component performance and availability. The specific alerts will be defined by the Services Provider contract with the State. |  |  |
| TST7 | 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. |  |  |
| TST8 | Solutions will assist the State in developing procedures to ensure that specified data is archived and protected from loss, unauthorized access, or destruction. |  |  |
| Transferability | | | |
| TRN1 | Hosting Service Provider will provide an exit plan addressing portability of Solution in case the State chooses to transition Environments to another Hosting Service Provider (see Transition Requirements). |  |  |
| TRN2 | Service Providers will describe the production support and transition approach and methodology used for transitioning out solutions. |  |  |
| TRN3 | 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. |  |  |
| TRN4 | Service Providers will incorporate the production support and transition approach into a comprehensive Production Support and Transition Plan complying with Solutions architectural design that describes solution and transition support over to the entity responsible for on-going production operations and support. |  |  |
| TRN5 | Service Providers will agree to continue normal operations activities until completion of Transition-Out Plan activities. |  |  |
| TRN6 | Shared Analytics Infrastructure Solutions will run on multiple Service Providers' hardware and operating systems, e.g., Oracle, IBM, HP, and Dell hardware, and AIX, Linux, Unix, and Windows Operating Systems. |  |  |
| TRN7 | Solutions will have a defined data migration strategy or process. |  |  |
| TRN8 | Solutions must supply ZTP (zero-touch-provisioning) so that data is easily transferred from one system to another without being required to re-enter data. |  |  |
| TRN9 | Solutions will support access from multiple channels and devices. |  |  |
| TRN10 | The solution provider must support Application-to-Application interfaces/integrations that must be quick and efficient, thus not negatively impacting user experience. |  |  |

**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) |  |  |
| 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 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, without including PII or other confidential information, 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) , without including PII or other confidential information, 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.**
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** |
| **Software** |  |  |  |  |  |  |
| Enterprise Application: License Fees | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| Maintenance &/or  License Fee Add-Ons | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| Subscription cost | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| Storage Limitations and/or Additional Fees | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| Database Software: License Fees | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| Middleware Tools: License Fees | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| Operating System Software: License Fees | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| Upgrade Costs for Later Years | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| Support and Maintenance Fees | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
|  | $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 or Integrate | $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 |
|  | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
|  | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| **Telecom** |  |  |  |  |  | $0.00 |
| Bandwidth | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
|  | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| **Hardware** |  |  |  |  |  | $0.00 |
| Computing Hardware | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| Storage and Backup Hardware | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| Network Hardware | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| Facilities/Data Center | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
|  | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
|  | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 | $0.00 |
| **Hosting** |  |  |  |  |  | $0.00 |
| Hosting Fees | $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** |  |  |  |  |  |

|  |  |
| --- | --- |
| **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).

**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** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

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:** |  |