**Appendix 3**

**Security and Vendor Questionnaire**

**Vendor Information**

**Vendor Legal Name:**

**Vendor Address:**

**Directions:**

Please fully complete this Security and Vendor Questionnaire (“Questionnaire”). This document is considered confidential, and your responses will be shared with only those state employees who need to know to properly vet you, the Vendor, and your proposed solution. This document will not be released to the public pursuant to SDCL 1-27-1.9. Below you will find specific instructions as to how to fill out this Questionnaire. Failure to fully respond to this Questionnaire will result in the State’s inability to properly vet you and your solution, which may impact the State’s ability to contract with you.

**Sections:**

You must answer all of the questions in the **System/Product-General** section regardless of your proposed hosting solution.

***NOTE:*** If your proposal includes options for more than one of the hosting sections below, please note how your answers in the System-General section would change depending upon the hosting solution.

Complete the following sections based upon your proposed hosting solution:

* **On-Prem**: If your proposal includes on-premises hosting (e.g. local install on a PC or server).
* **State Cloud Hosted**: If your proposal includes hosting on the State's cloud platform.
* **Vendor Hosted**: If your proposal includes hosting your solution or State Data on a cloud platform that is not the State’s cloud platform (e.g. hosted in Vendor’s data centers or hosted on Vendor instance of AWS).

**Response Guidance:**

* **Grayed-out Cells**: Cells that are grayed out require more than a simple "Yes/No/NA" answer. Please provide a more comprehensive response.
* NA (Not Applicable): If a question does not pertain to your product or service, please indicate "NA."
* Explanation: For most questions, a detailed explanation of your response will provide valuable insight. The more information you provide, the better we can understand your technology.
* References: If your answer references another document or section of your RFP response, please provide the name of the document, the specific page number, and the paragraph.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **System/Product – General**  **No matter which hosting section you will be completing, you must answer all questions is in this section. If you are proposing two options for hosting, please note how your answers in this section would change depending upon which hosting option is chosen by the State.** | | | | |
| **Response** | | | | |
| **Category** | **#** | **Question** |  | **Mark all that apply:** |
| **System** |  | What is your proposed solution(s)? | Vendor Hosted Solution |  |
| PaaS Solution in the State’s Cloud |  |
| On-Prem Solution |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Cost** | 1 | Please list any required license information for software/devices connected to state devices. |  |  |  |  |
| 2 | Are all costs that are incurred by the State reflected in the cost proposal? Applicable costs for hosting, software, and licensing should be itemized. Any increases in cost should be detailed in the cost proposal for all years of the contract. |  |  |  |  |
| 3 | Are all costs for your software licenses in addition to third-party software (For example: MS-SQL, MS Office, Oracle) included in your cost proposal? |  |  |  |  |
| 4 | If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Infrastructure** | 1 | Does the proposed solution include the use of email? |  |  |  |  |
| 2 | Will the vendor be providing the email service as part of the project? |  |  |  |  |
| 3 | Is there an expectation that email come from the State’s domain? |  |  |  |  |
| 4 | Will the system involve the use of bulk email distribution? |  |  |  |  |
| 5 | Does the solution have mitigations to prevent blacklisting due to high message volume? |  |  |  |  |
| 6 | Specify the type of access required by the proposed solution to state hosted resources. (For example: VPN, API, SFTP, Other) |  |  |  |  |
| 7 | To fulfill the scope of work and facilitate connection to other applications or data, will the State/external vendors be required to develop deliverables such as custom interfaces, reports, and data extractions? |  |  |  |  |
| 8 | Will you provide any APIs that the State can or will use? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Identity and Access Management** | 1 | Does the solution require user authentication? |  |  |  |  |
| 2 | If the solution requires user authentication, how does the solution support OpenID Connect (OIDC) or OAuth protocols to meet the State's Single Sign-On requirements? |  |  |  |  |
| 3 | If the solution requires user authentication, describe how users are onboarded/provisioned, offboarded/disabled, and managed in the system. |  |  |  |  |
| 4 | If you do not support OIDC or OAuth protocols, is the login name customizable? |  |  |  |  |
| 5 | If you do not support OIDC or OAuth protocols, what mitigations do you have in place to prevent brute force attacks? |  |  |  |  |
| 6 | If you do not support OIDC or OAuth protocols, are account credentials hashed and encrypted when stored? |  |  |  |  |
| 7 | If yes, please describe the encryption used (e.g. SHA256). |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Application Development** | 1 | Do you use any of the following development technologies for your solution? |  |  |  | **If marked yes, please indicate the version.** |
| .NET/.NET Framework |  |  |  |  |
| Java/JSP |  |  |  |  |
| React |  |  |  |  |
| Node |  |  |  |  |
| Angular |  |  |  |  |
| Python |  |  |  |  |
| PHP |  |  |  |  |
| Other (Please list): |  |  |  |  |
| 2 | Will your system use Adobe Air, Adobe Flash, Adobe ColdFusion, Apache Flex, Microsoft Silverlight, Perl, Magento, or QuickTime? If yes, explain? |  |  |  |  |
| 3 | If the State of South Dakota will gain ownership of the deliverables or source code, does the proposal include a knowledge transfer plan? |  |  |  |  |
| 4 | Are static or dynamic software security analysis tools used to identify weaknesses in the software that can lead to exploitable vulnerabilities? |  |  |  |  |
| 5 | If yes, which tools are used? |  |  |  |  |
| 6 | What classes of weaknesses are covered? |  |  |  |  |
| 7 | When in the Software Development Life Cycle (SDLC) are these scans performed? |  |  |  |  |
| 8 | Are security experts involved in the analysis of the scan results? |  |  |  |  |
| 9 | If part of the deliverables is a website or a web application, please describe your conformance with the Americans with Disability Act and the Web Content Accessibility Guidelines (WCAG). |  |  |  |  |
| 10 | What version of WCAG are you compliant with and at what level? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Security Posture** | 1 | What security criteria are considered when selecting third party suppliers? |  |  |  |  |
| 2 | How do you ensure your suppliers maintain an industry standard level of security? |  |  |  |  |
| 3 | Does your software contain any third-party developed components including open- source software or libraries? |  |  |  |  |
| 4 | If yes, do you check for vulnerabilities in your software or library that are listed in: |  |  |  |  |
| a. Common Vulnerabilities and Exposure (CVE) database? |  |  |  |  |
| b. Open Web Application Security Project (OWASP) Top Ten? |  |  |  |  |
| 5 | Have you ever had unauthorized access to your systems or client data? If so, provide detailed information. |  |  |  |  |
| 6 | Do you have any security certification? (For example: StateRAMP, FedRAMP, or HITRUST) If yes, please list. |  |  |  |  |
| 7 | Please describe the scope and give an overview of the content of the security training you require of your staff, include how often the training is given and to whom. |  |  |  |  |
| 8 | How does the software’s exception handling mechanism ensure that faults do not leave the software, its resources, or its data (both in memory and on disk) in an insecure or unstable state? |  |  |  |  |
| 9 | Please describe how and where the software validates inputs from untrusted sources, such as through whitelisting or other filtering methods before these inputs are used. |  |  |  |  |
| 10 | Does the program utilize runtime security defenses such as address space randomization, stack overflow protection, prevention of execution from data memory, and taint checking? |  |  |  |  |
| 11 | What anti-malware product(s) do you use to secure your organization? |  |  |  |  |
| 12 | Are any of the deliverables or services provided by you manufactured in or provided by a banned entity, as determined by the federal government or any state government (e.g. China, North Korea, Iran, Huawei Technologies Company, ZTE Corporation)? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Auditing** | 1 | Please list the types of event logs you keep and how long you keep them. |  |  |  |  |
| 2 | How are security logs and audit trails protected from tampering or modification? |  |  |  |  |
| 3 | Has the software been assessed against any formal evaluation process? (For example: Common Criteria or FIPS) If yes, please provide an evaluation report. |  |  |  |  |
| 4 | Will the proposed solution provide the capability to audit user activity by action, person, date, and time? |  |  |  |  |
| 5 | Does your company have a SOC 2 Type II audit report? |  |  |  |  |
| 6 | If yes, will you provide a copy of your latest report? |  |  |  |  |
| 7 | Is the audit performed annually? |  |  |  |  |
| 8 | Does your company have any real-time security auditing processes? |  |  |  |  |
| 9 | Does your company, or a third-party, perform site inspections/policy compliance audits of your development facilities? |  |  |  |  |
|  | 10 | If yes, how often do these inspections / audits occur? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Hosting** | 1 | The State of South Dakota currently schedules routine maintenance from 0400 to 0700 on Tuesday mornings for our non-mainframe environments and once a month from 0500 to 1200 for our mainframe environment. Systems may be offline during this scheduled maintenance time periods. Will this have a detrimental effect to the system? |  |  |  |  |
| 2 | Please provide documentation on the deployment of your proposed solution, including server configuration and hardening, software installed on servers, and software/peripherals to be installed/connected to workstations. |  |  |  |  |
| 3 | If a Database is required, what technology will be used (i.e.  Microsoft SQL Server, Oracle, MySQL)? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Networking** | 1 | It is State policy that all access from outside of the State of South Dakota’s private network will be limited to set ports as defined by the State and all traffic leaving or entering the State network will be monitored. Would this affect the implementation of the system? If yes, explain. |  |  |  |  |
| 2 | It is State policy that no equipment can be connected to State Network without direct approval of BIT. Would this affect the implementation of the system? If yes, explain. |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Privacy** | 1 | Will the State’s data be used for any purpose other than South Dakota’s usage? |  |  |  |  |
| 2 | Will organizations other than the State of South Dakota have access to our data? |  |  |  |  |
| 3 | Do you have a device policy that prohibits your staff from putting any sort of sensitive or legally protected State data on non-company owned device or system? |  |  |  |  |
| 4 | Does the system offer internet security for public portals through TLS, in accordance with the latest OWASP recommendations? |  |  |  |  |
| 5 | Will this traffic be decrypted and inspected? |  |  |  |  |
| 6 | Do you use Content Threat Removal to extract and transform data? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Threat Management** | 1 | Have you ever issued any cybersecurity advisories for any of your deliverables? If so, please give the history of cybersecurity advisories issued by you. Include the deliverable name, date, and the nature of the cybersecurity advisory. |  |  |  |  |
| 2 | The protection of the State’s system and data is of utmost importance. Web Application Vulnerability Scans must be done if:  • An application will be placed on the State’s system.  • The State’s system connects to another system.  • The contractor hosts State data.  • The contractor has another party host State data the State will want to scan that party.  The scanning will be done with industry standard tools that check against OWASP Top 10 and other common web application vulnerabilities. The State will want to scan a non-production environment which is identical to production. Scanning will also be required, at a minimum, annually as well as when there are code changes.  Will you allow the State to scan a non-production environment of the web application(s) and APIs that will handle State data? If no, please explain your vulnerability management process for your proposed solution. |  |  |  |  |
| 3 | Has the software been assessed for publicly known vulnerabilities and/or attack patterns identified in the Common Vulnerabilities & Exposures (CVE®) or Common Weakness Enumerations (CWEs)? If yes, how have the findings been mitigated? |  |  |  |  |
| 4 | Has the product undergone any penetration testing? If yes, how frequently, by whom, and are the test reports available under a nondisclosure agreement? |  |  |  |  |
| 5 | How have the findings been mitigated? |  |  |  |  |
| 6 | What are the policies and procedures used to protect State information from unauthorized access? How are the policies enforced? |  |  |  |  |
| 7 | What are your procedures for intrusion detection, incident response, and incident investigation and escalation? |  |  |  |  |
| 8 | How do you monitor your application, systems, and data center for security events, incidents, or information? |  |  |  |  |
| 9 | How are enhancement requests and reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, prioritized, and reported? |  |  |  |  |
| 10 | Have you performed an information security risk assessment? |  |  |  |  |
| 11 | If yes, how often are these performed, and will you share the information security risk assessment report(s) with us? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **End-Point Management** | 1 | What end user operating system(s) does your proposed solution support? |  |  |  |  |
| 2 | Does the solution include a mobile-native application? |  |  |  |  |
| 3 | Will the system data be exportable by the user to tools like Excel or Access? |  |  |  |  |
| 4 | Is this a browser-based user interface? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **IoT/Peripherals** | 1 | Are you providing a device or software that can be defined as being Internet of Thing (IoT) to be installed on the State’s network? Examples include IP camera, network printer, or connected medical device. |  |  |  |  |
| 2 | If yes, what is your process for ensuring the software on your IoT devices are maintained or updated? |  |  |  |  |
| 3 | How do you secure and update Internet of Things (IoT) devices on the Vendor’s network? |  |  |  |  |
| 4 | Please list any changes or additions to State devices or network connectivity required, for example: software installs, license monitoring software, connecting peripheral devices (wired or wireless), policies, browser extensions, to implement your proposed solution? |  |  |  |  |
| 5 | Will the system print to a Citrix compatible networked printer? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Vendor Processes** | 1 | What kind of technical support, installation help, documentation, or assistance do you offer? |  |  |  |  |
| 2 | Is on-site assistance available? |  |  |  |  |
| 3 | If yes, are there any charges for the on-site assistance? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Business Processes** | 1 | Explain the change management procedure used to identify the type and extent of changes allowed in the software throughout its lifecycle. Include information on the oversight controls for the change management procedure. |  |  |  |  |
| 2 | What security design and security architecture documents are prepared as part of the SDLC process? How are they maintained? Are they available to/for review? |  |  |  |  |
| 3 | Does your organization incorporate security risk management activities as part of your software development methodology? If yes, please provide a copy of this methodology or provide information on how to obtain it from a publicly accessible source. |  |  |  |  |
| 4 | Please describe any resources or services which are provided as a part of the solution that are located outside of the jurisdiction of the United States. |  |  |  |  |
| 5 | Please provide your privacy policy that covers sharing data with other entities or other jurisdictions. |  |  |  |  |
| 6 | Please describe any resources or services that are subcontracted to a third party. |  |  |  |  |
| 7 | What is your process for applying patches to the proposed solution? Please include client communication plans, expected downtime policies, and update reversion capabilities. |  |  |  |  |
| 8 | Please provide the disaster recovery plan that applies to the proposed solution. Please include strategies to mitigate unplanned disruptions, actions required to recover the solution, data backup policies and procedures, whether the recovery includes warm or hot backups, and the expected RTO and RPO. |  |  |  |  |
| 9 | Will the proposed solution provide an archival solution to meet the State’s record retention requirements or is the State expected to develop a customized archival solution? |  |  |  |  |
| 10 | Would you be willing to undergo fingerprint-based background checks? If no, you must provide your background check policy. |  |  |  |  |
| 11 | Will the State of South Dakota own the data in the proposed solution? |  |  |  |  |
| 12 | Is the controlling share (51%+) of your company owned by one or more non-U.S. entities? |  |  |  |  |
| 13 | What are your record retention capabilities? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Artificial Intelligence** | 1 | Does you company integrate Artificial Intelligence (AI) or AI tools into your product offerings or development process? |  |  |  |  |
| 2 | If yes, where does your company plan to integrate AI decision making or processing to the product we are receiving? |  |  |  |  |
| 3 | If yes, how do you assure that the company’s use of AI during the development lifecycle of this product does not expose the product’s intellectual property (IP) regarding security, algorithms, or functionality to third parties? |  |  |  |  |
| 4 | If yes, please provide the AI product(s) used in your software development lifecycle and whether by contract your use of those products is used to train the AI product. (Provide the name of the product and evidence that it does not retain nor get trained by the data your development provides AI via prompts or other interactions.) |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **On-Prem**  **The following questions must be answered if your proposed solution will be hosted On-Prem.** | | | | | | |
| **Response** | | | | | | |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Infrastructure** | 1 | Can your system be run behind load balancers and handle SSL off-loading? |  |  |  |  |
| 2 | Will the system infrastructure include a separate OLTP or Data Warehouse Implementation? |  |  |  |  |
| 3 | Will the system infrastructure have a special backup requirement? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Security Posture** | 1 | The State implements enterprise-wide anti-virus solutions on all on-prem servers and workstations as well as controls the roll outs of any and all Microsoft patches based on level of criticality. Do you have any concerns regarding this process? |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** | |
| **Hosting** | 1 | It is State policy that all Contractor Remote Access to systems for support and maintenance on the State Network will only be allowed through Citrix Netscaler.  What type of access is required by vendor to maintain and support the solution? |  |  |  | Please select which applies: | |
| Not Required |  |
| Citrix |  |
| Other |  |
| If other, please explain: | |
| 2 | What physical access do you require to work on hardware? |  |  |  |  | |
| 3 | The State maintains standards for software versions in use on state devices. Does the proposed solution support at least the following (as required): |  |  |  |  | |
| Windows Server 2022 |  |  |  |  | |
| IIS (version from 2022) |  |  |  |  | |
| MS SQL Server 2016 Standard Edition |  |  |  |  | |
| VMWare 7 |  |  |  |  | |
| 4 | The State normally updates the Windows operating system starting the 3rd Tuesday of each month. Would this have any expected impact on the proposed solution? |  |  |  |  | |
| 5 | The State reserves the right to migrate virtual machines to different hosts, to support availability, load, and recovery. Will this impact the proposed solution? |  |  |  |  | |
| 6 | The State has a virtualize first policy that requires all new systems to be configured as virtual machines. Would this affect the implementation of the system? If yes, explain. |  |  |  |  | |
| 7 | Does your application use any Oracle products? |  |  |  |  | |
| 8 | If yes, what product(s) and version(s)? |  |  |  |  | |
| 9 | Do you have support agreements for these products? |  |  |  |  | |
| 10 | Will your application require a dedicated environment? |  |  |  |  | |
| 11 | Will there be a request to include an application to monitor license compliance? |  |  |  |  | |
| 12 | Will the system infrastructure have any processes that require scheduling? |  |  |  |  | |
| 13 | Do you have agents or scripts which execute on servers of hosted applications? If yes, what are the procedures for reviewing the security of those scripts and agents? |  |  |  |  | |
| 14 | How many of the vendor’s staff will need access to the state system and what level of access will they require? |  |  |  |  | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Networking** | 1 | The system must use network communications compliant with the Institute of Electrical and Electronics Engineers (IEEE) standard TCP/IP (IPv4, IPv6). It must use standard Internet Protocol ports, not dynamic TCP or UDP ports, unless the system is well-known and state firewall-supported (HTTPS, SSH, SFTP, etc.). Would this affect the system's implementation? If yes, explain. |  |  |  |  |
| 2 | It is State policy that all systems must be compatible with BIT’s dynamic IP addressing solution (DHCP). Would this affect the implementation of the system? If yes, explain. |  |  |  |  |
| 3 | It is State policy that systems must support Network Address Translation (NAT) and Port Address Translation (PAT) running inside the State Network. Would this affect the implementation of the system? If yes, explain. |  |  |  |  |
| 4 | Please describe the types and levels of network access your system/application will require. This should include, but not be limited to TCP/UDP ports used, protocols used, source and destination networks, traffic flow directions, who initiates traffic flow, whether connections are encrypted or not, and types of encryption used. The Contractor should specify what access requirements are for user access to the system and what requirements are for any system level processes. The Contractor should describe all requirements in detail and provide full documentation as to the necessity of the requested access. |  |  |  |  |
| 5 | All network hardware must operate within the current configurations of the State of South Dakota’s firewalls, switches, IDS/IPS, and desktop security infrastructure. Would this affect the implementation of the proposed solution? If yes, explain. |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **State Cloud**  **The following questions must be answered if your proposed solution will be hosted in the State Cloud.** | | | | | | | |
| **Response** | | | | | | | |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** | |
| **Hosting** | 1 | What type of access is required by vendor to maintain and support the solution? |  |  |  | Please select which applies: | |
| Not Required |  |
| State Cloud Access |  |
| Other |  |
| If other, please explain: | |
| 2 | How many of the vendor’s staff will need access to the state system and what level of access will they require? |  |  |  |  | |
| 3 | Will the system infrastructure include a separate Online Transaction Processing (OLTP) or Data Warehouse Implementation? |  |  |  |  | |
| 4 | Will the system infrastructure have a special backup requirement? |  |  |  |  | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Networking** | 1 | How do you perform analysis against the network traffic being transmitted or received by your application, systems, or data center? |  |  |  |  |
| 2 | What benchmarks do you maintain and monitor your systems against for network usage and performance? |  |  |  |  |
| 3 | What process(es) or product(s) do you use to complete network traffic analysis, and what results or process(es) can you share? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Vendor Hosted**  **The following questions must be answered if your proposed solution will be hosted by you or a third-party hosting provider of your choosing.** | | | | | | |
| **Response** | | | | | | |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Hosting** | 1 | Are you hosting the proposed solution, or will it be hosted by a third party? (For example, AWS, Azure). If a third party is hosting, please identify. |  |  |  |  |
| 2 | Where are your data centers located (Please include locations for disaster recovery)? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Networking** | 1 | How do you perform analysis against the network traffic being transmitted or received by your application, systems, or data center? |  |  |  |  |
| 2 | What benchmarks do you maintain and monitor your systems against for network usage and performance? |  |  |  |  |
| 3 | What process(es) or product(s) do you use to complete network traffic analysis, and what results or process(es) can you share? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Privacy** | 1 | Please explain how the State’s data is kept separate from other organization’s data. |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Vendor Processes** | 1 | Do you require multifactor authentication be used by employees and subcontractors who have potential access to legally protected State data or administrative control? |  |  |  |  |
| 2 | If no, do you plan on implementing multifactor authentication? If so, when? |  |  |  |  |
| 3 | If yes, please explain your practices on multifactor authentication including the authenticator level used as defined in NIST 800-63 in your explanation. |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **#** | **Question** | **Yes** | **No** | **NA** | **Explain your response.** |
| **Business Processes** | 1 | Provide your procedures and policies for media sanitization. |  |  |  |  |