* 1. Hosting and Data Access Requirements

The contract doubles as an agreement for the State to own the data tables and is able to manipulate data, run reports as needed, pull code tables, access raw data, and develop dashboards as needed through Microsoft Power BI, ESRI, Tableau and associated platforms.

* 1. Single Sign-On Requirements

As part of the State’s Identity and Access Management (IAM) strategy, the proposed solution will need to integrate with the State of South Dakota’s standard identity management service single sign-on (SSO) which enables custom control of how citizens and state employees sign up, sign in, and manage their profiles.

The SSO supports two industry standard protocols: OpenID Connect and OAuth 2.0 (preferred). This identity management will handle password recovery and multi-factor authentication (MFA). MFA is required for all application Administrators and may be required for other users. Microsoft’s official documentation on the identity provider the State has implemented can be found at: 1) <https://docs.microsoft.com/en-us/azure/active-directory-b2c/> and <https://docs.microsoft.com/en-us/azure/active-directory-b2c/integrate-with-app-code-samples> for public/citizens (Azure B2C), 2) <https://learn.microsoft.com/en-us/azure/active-directory/architecture/auth-oauth2> and <https://learn.microsoft.com/en-us/azure/active-directory/develop/v2-protocols-oidc> for state employees, businesses, partners, providers, etc. (Azure Active Directory).

**If the offeror is not able to fulfill this identity management standard, they will be excluded from the list.**

* 1. Onboarding/Provisioning Users

The offeror must describe how new users are onboarded/provisioned in the system using an external identity provider and provide an Identity/SSO/Login Design Document.

* 1. Interfaces and Integration

The offeror must describe how the system can adapt to business necessary interfaces using widely adopted open APIs and standards. Additionally,       expects that the offeror will make available/expose software services and publish documentation for those software services that would enable third party developers to interface other business applications. A detailed description of system capability must be included in the proposal.

* 1. Solution Diagram

The offeror must provide a solution diagram providing specific details of how the entire solution will meet the requirements of the RFP. This will include integration with the State’s infrastructure, existing systems that will integrate with the proposed solution, how data would flow between systems, the technology stack of the solution including any dependencies, and include, but not be limited to, user onboarding/provision and SSO.

# **Project Deliverables/Approach/Methodology**

If the State will be hosting the solution the offeror will provide a system diagram. The diagram must be detailed enough that the State can understand the components, the system flow, and system requirements. It is preferred that the diagram be provided as a separate document or attachment. The file must be named “(Your Name) System Diagram and Requirements”. If the offeror elects to make the diagram part of the proposal, then the location of the diagram must be clearly indicated in the Table of Contents.

If the offeror is hosting the solution, provide a diagram giving an overview of the proposed system. It is preferred that this diagram be provided as a separate document or attachment. The file must be named “(Your Name) Hosted System Diagram”. If the offeror elects to make the diagram part of the proposal, then the location of the diagram must be clearly indicated in the Table of Contents.

The offeror should state whether its proposed solution will operate in a virtualized environment. Offeror also should identify and describe all differences, restrictions or limitations of its proposed solution with respect to operation, licensing, support, certification, warranties, and any other details that may impact its proposed solution when hosted in a virtualized environment. This information must be included with the solution diagram for the offeror hosted solution.

This section identifies tasks and deliverables of the project as described in Section 3 above. The selected offeror is responsible for providing the required deliverables. These deliverables will be the basis against which the offeror’s performance will be evaluated.

The offeror is required to include a test system for its application. This test system will be used at the discretion of BIT. All resource costs associated with keeping the test system available must be borne by the project owner or the offeror. Any licensing costs for the test system must be included with the costs.

At BIT’s discretion, any code changes made by the offeror, either during this project or thereafter, will be placed in the above test system first. It is at BIT’s discretion if the code changes are applied by BIT or the offeror. If the code testing delays a project’s timeline, a change management process should be followed, and the State will not be charged for this project change. If the test and production systems are to be hosted by the State, the schedule for the testing of the code changes is to be decided by BIT. Testing of emergency code changes will be scheduled by BIT based on the severity and resource availability.

The test system will be maintained by the offeror as a mirror image of the production system code base. At BIT’s discretion, updates to the production system will be made by copying code from the test system after the test system passes BIT certification requirements.

If BIT determines that the application must be shut down on the production system, for any reason, the offeror will, unless approved otherwise by BIT, diagnosis the problem on and make all fixes on the test system. The offeror is expected to provide proof, to BIT, of the actions taken to remediate the problem that led to the application being denied access to the production system before the application can go back into production. This proof can be required by BIT even if the fix passes all BIT certification criteria. BIT is willing to sign a non-disclosure agreement with the offeror if the offeror feels that revealing the fix will put the offeror’s intellectual property at risk.

All solutions acquired by the State that are hosted by the offeror, including Software as a Service, or hosted by a third-party for the offeror will be subjected to security scans by BIT or preapproved detailed security scan report provided by the offeror. The scan report sent in with the proposal can be redacted by the offeror. The State’s goal at this point is to see if the contents of the report will be acceptable, not to review the contents themselves. If the offeror will be providing a security scan report, one must be sent with the proposal for approval. Approval is not guaranteed. If the scan report is not acceptable, the State must scan the offeror’s solution. The actual scanning by the State or the submission of a security scan report will be done if the proposal is considered for further review. A detailed security report must consist of at least:

* The system that was evaluated (URL if possible, but mask it if needed).
* The categories that were evaluated (example: SQL injection, cross site scripting, etc.)
* What were the general findings, (meaning how many SQL injection issues were found, what was the count per category)
* Technical detail of each issue found. (where was it found – web address, what was found, the http response if possible)

The cost of any scans done by the offeror or the offeror’s costs associated with the State’s scans must be part of the offeror’s bid. If the offeror is sending a security scan report, it should price the product both as if the State was to do the security scan or if the offeror was to do the security scan.

All hardware, website(s), or software purchased by the State and hosted by the State will be subjected to security scans by BIT.

Security scanning will be performed during the software development phase and during pre-production review. These scans and tests can be time consuming and should be allowed for in project planning documents and schedules. Products that do not meet BIT’s security and performance requirements will not be allowed to go into production and may be barred from UAT until all issues are addressed to the State’s satisfaction. The State urges the use of industry scanning/testing tools and secure development methods be employed to avoid unexpected costs and project delays. Costs to produce and deliver secure and reliable applications are the responsibility of the software entity producing or delivering an application to the State. Unless expressly indicated in writing, the State assumes all price estimates and bids are for the delivery and support of applications and systems that will pass security and performance testing. If the State determines the hardware, website(s), software, and or cloud services have security vulnerabilities that must be corrected, the State will inform the offeror of the nature of the issue and the offeror will be required to respond in writing regarding mitigation plans for the security vulnerabilities. If the product(s) does not pass the initial security scan, additional security scans may be required to reach an acceptable level of security. The offeror must pass a final follow-up security scan for the website(s), software or cloud services for the product(s) to be acceptable products to the State. The State may suspend or cancel payments for hardware, website(s), software, or cloud services that do not pass a final security scan.

Any website or web application hosted by the offeror that generates email cannot use “@state.sd.us” as the originating domain name per state security policy.

As part of this project, the offeror will provide a monitoring tool the State can utilize to monitor the operation of the proposed solution as well as all systems and all subcomponents and connections. It is required that this tool be easy to use and provide a dashboard of the health of the proposed solution. The effectiveness of this monitoring tool will be a component of the acceptance testing for this project.

As part of the project plan, the offeror will include development of an implementation plan that includes a back out component. Approval of the implementation plan by BIT should be a project milestone. Should the implementation encounter problems that cannot be resolved and the implementation cannot proceed to a successful conclusion, the back out plan will be implemented. The Implementation and back out documentation will be included in the project documentation.

The successful offeror will use the approved BIT processes and procedures when planning its project, including BIT’s change management process. Work with the respective agency’s BIT Point of Contact on this form. The Change Management form is viewable only to BIT employees. The purpose of this form is to alert key stake holders (such as: Operations, Systems Support staff, Desktop Support staff, administrators, Help Desk personnel, client representatives, and others) of changes that will be occurring within state resources and systems to schedule the:

* Movement of individual source code from test to production for production systems
* Implementation of a new system
* A major enhancement to a current system or infrastructure changes that impact clients
* Upgrades to existing development platforms

If as part of the project the state will be acquiring software the proposal should clearly state if the software license is perpetual or a lease. If both are options, the proposal should clearly say so and state the costs of both items separately.

Include in your submission details on your:

* Data loss prevention methodology;
* Identity and access management;
* Security intelligence;
* Annual security training and awareness;
* Manual procedures and controls for security;
* Perimeter controls;
* Security certifications and audits.

If the offeror will have State data on its system(s) or on a third-party’s system and the data cannot be sanitized at the end of the project, the offeror’s proposal must indicate this and give the reason why the data cannot be sanitized as per the methods in NIST 800-88.

The offeror’s solution cannot include any hardware or hardware components manufactured by Huawei Technologies Company, Nuctech, or ZTE Corporation or any subsidiary or affiliate of such entities. This includes hardware going on the State’s network as well as the offeror’s network if the offeror’s network is accessing the State’s network or accessing State data. This includes Infrastructure as a Service, Platform as a Service or Software as a Service situations. Any company that is considered to be a security risk by the government of the United States under the International Emergency Economic Powers Act, in a United States appropriation bill, an Executive Order, or listed on the US Department of Commerce’s Entity List will be included in this ban.

If the offeror’s solution requires accounts allowing access to State systems, then the offeror must indicate the number of the offeror’s staff or subcontractors that will require access, the level of access needed, and if these accounts will be used for remote access. These individuals will be required to use Multi-Factor Authentication (MFA). The State’s costs in providing these accounts will be a consideration when assessing the cost of the offeror’s solution. If the offeror later requires accounts that exceed the number of accounts that was originally indicated, the costs of those accounts will be borne by the offeror and not passed onto the State. All State security policies can be found in the Information Technology Security Policy (ITSP) attached to this RFP. The offeror should review the State’s security policies regarding authorization, authentication, and, if relevant, remote access (See ITSP 230.67, 230.76, and 610.1). Use of Remote Access Devices (RAD) by contractors to access the State’s system must be requested when an account is requested. The offeror should be aware that access accounts given to non-state employees, Non-State (NS) accounts, will be disabled if not used within 90 days. A NS account may be deleted after 30 days if it is not used.

**Testing:** If the software is being hosted on the state systems, regression testing, and integration testing is done by the contractor with assistance of BIT Development. If the software is being hosted on the state systems, functional testing is generally done by the contractor and the agency with assistance of BIT Development. If the software is being hosted on the state systems, performance testing and load testing is generally done by BIT Telecommunications division. If the contractor is hosting the software on its systems, regression testing, if relevant, integration testing, if relevant, functional testing, performance and load testing should be done by the contractor. The UAT is generally done by the contractor and the agency, whether the software is hosted on the State’s or the contractor’s systems. All testing is done in test environments either set up by the contractor or by BIT. All test results should meet the requirements of the agency before the software goes into production. For a software development project when the software is being customized, at a minimum, regression, integration, functional, and UAT tests must be done. If software is being developed fresh, at a minimum, integration, functional, and UAT tests must be done. How extensive the testing would be could vary with the criticality or complexity of an application. If you are unsure of the types of testing that should be done, bring the question up at the client planning meeting for the RFP. If performance and load tests are not done, then you are accepting the risk that your application may not perform as fast, do the amount of work you would like, or not operate under all the conditions you would want. Assuming no problems are found, you should plan on a minimum of three weeks for performance and load testing if done by BIT. There have been contractors on major projects that have had the attitude that if a project falls behind, the best way to make up the time is to reduce the testing, most commonly the performance and load testing. Be aware of the risks you run if this is proposed to you.

**Regression Testing**- Regression testing is the process of testing changes to computer programs to make sure that the older programming still works with the new changes.

**Integration Testing**- Integration testing is a software development process which program units are combined and tested as groups in multiple ways. In this context, a unit is defined as the smallest testable part of an application. Integration testing can expose problems with the interfaces among program components before trouble occurs in real-world program execution. Integration testing is also known as integration and testing (I&T).

**Functional Testing**- Functional testing is primarily used to verify that a piece of software is meeting the output requirements of the end-user or business. Typically, functional testing involves evaluating and comparing each software function with the business requirements. Software is tested by providing it with some related input so that the output can be evaluated to see how it conforms, relates or varies compared to its base requirements. Moreover, functional testing also checks the software for usability, such as ensuring that the navigational functions are working as required. Some functional testing techniques include smoke testing, white box testing, black box testing, and unit testing.

**Performance Testing**- Performance testing is the process of determining the speed or throughput of an application. This process can involve quantitative tests such as measuring the [response time](http://searchnetworking.techtarget.com/definition/response-time) or the number of [MIPS](http://searchdatacenter.techtarget.com/definition/MIPS) (millions of instructions per second) at which a system functions. Qualitative attributes such as [reliability](http://whatis.techtarget.com/definition/reliability), [scalability](http://searchdatacenter.techtarget.com/definition/scalability) and [interoperability](http://searchsoa.techtarget.com/definition/interoperability) may also be evaluated. Performance testing is often done in conjunction with [load testing](http://searchsoftwarequality.techtarget.com/definition/stress-testing).

**Load Testing**-Load testing is the process of determining the ability of an application to maintain a certain level of effectiveness under unfavorable conditions. The process can involve tests such as ramping up the number of users and transactions until the breaking point is reached or measuring the frequency of errors at your required load. The term also refers to qualitative evaluation of factors such as [availability](http://searchnetworking.techtarget.com/definition/availability) or resistance to denial-of-service (DoS) attacks. Load testing is often done in conjunction with the more general process of [performance testing](http://searchsoftwarequality.techtarget.com/definition/performance-testing). Load testing is also known as stress testing.

**User Acceptance Testing**- User acceptance testing (UAT) is the last phase of the software testing process. During UAT, actual software users test the software to make sure it can handle required tasks in real-world scenarios, according to specifications. UAT is one of the final and critical software project procedures that must occur before newly developed or customized software is rolled out. UAT is also known as beta testing, application testing or end user testing. In some cases, UAT may include piloting of the software.

The State, at its sole discretion, may consider a solution that does include all or any of these deliverables or consider deliverables not originally listed. An offeror **must** highlight any deliverable it does not meet and give any suggested “work-around” or future date that it **will** be able to provide the deliverable.

## **Non-Standard Hardware and software**

## State standard hardware and software should be utilized unless there is a reason not to. If your proposal will use non-standard hardware or software, you must first obtain State approval. If your proposal recommends using non-standard hardware or software, the proposal should very clearly indicate what non-standard hardware or software is being proposed and why it is necessary to use non-standard hardware or software to complete the project requirements. The use of non-standard hardware or software requires use of the State’s New Product Process. This process can be found through the Standards’ page and must be performed by State employees. The costs of such non-standard hardware or software should be reflected in your cost proposal. The work plan should also account for the time needed to complete the New Product Process. See <https://bit.sd.gov/bit?id=bit_standards_overview>, for lists of the State’s standards. The proposal should also include a link to your hardware and software specifications.

If non-standard hardware or software is used, the project plan and the costs stated in Section 7 must include service desk and field support, since BIT can only guarantee best effort support for standard hardware and software. If any software development may be required in the future, hourly development rates must be stated. The project plan must include the development and implementation of a disaster recovery plan since non-standard hardware and software will not be covered by the State’s disaster recovery plan. This must also be reflected in the costs.

The offeror must complete the list of technical questions, Security and Vendor Questions which is attached as Appendix B. These questions and the offeror’s responses may be used in the proposal evaluation.

* 1. **BACKGROUND CHECKS**

The offeror must include the following statement in its proposal:

(Company name here) acknowledges and affirms that it understands that the (company name here) employees who have access to production Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI), any information defined under state statute as confidential or have access to secure facilities will have fingerprint-based background checks. These background checks will be used to check the criminal history records of the State as well as the Federal Bureau of Investigation’s records. (Company name here) acknowledges and affirms that this requirement will extend to include any Subcontractor’s, Agents, Assigns and or Affiliated Entities employees.