STATE OF SOUTH DAKOTA
DEPARTMENT OF CORRECTIONS
3200 E HWY 34
PIERRE, SOUTH DAKOTA 57501

South Dakota Department of Corrections Website Redevelopment & Maintenance to include:
redevelopment and construction of a new website as well as the intranet,
user testing & maintenance.

PROPOSALS ARE DUE NO LATER THAN JUNE 9, 2023

RFP#: 23RFP8586 CONTACT: Danna.Humig@state.sd.us EMAIL: Danna.Humig@state.sd.us

READ CAREFULLY

FIRM NAME: ______________________ AUTHORIZED SIGNATURE: ____________________

ADDRESS: ______________________ TYPE OR PRINT NAME: ____________________

CITY/STATE: ______________________ TELEPHONE NO: ____________________

ZIP (9 DIGIT): ______________________

FEDERAL TAX ID#: ______________________ E-MAIL: ____________________

PRIMARY CONTACT INFORMATION

CONTACT NAME: ______________________ TELEPHONE NO: ____________________

______________________ E-MAIL: ____________________

1.0 GENERAL INFORMATION

1.1 BIT SECURITY STANDARDS

Any contract or agreement resulting from this RFP will need to incorporate and conform to the necessary security standards required by the South Dakota Bureau of Information and Telecommunications (BIT). In addition, any contract or agreement resulting from this RFP will include the State's standard I/T contract terms listed in Attachment A and the State's standard contract terms and conditions as identified in Section 2.0 below, along with any additional contract terms as negotiated by the parties. As part of the negotiation process the contract terms listed in Attachment A may be altered or deleted. The vendor must indicate in its response any issues it has with specific contract terms. If the vendor does not indicate that there are any issues with any contract terms, then the State will assume those terms are acceptable to the vendor. There is also a list of technical questions, Security and Vendor Questions which is attached as Attachment B, the vendor must complete. These questions may be used in the proposal evaluation. It is preferred that the vendor's response to these questions is provided as a separate document from the RFP response. If the vendor will be hosting the solution, the file name must be "(Your Name) Hosted Security and Vendor Questions Response". If the solution will be hosted by the State, the file must be named "(Your Name) Security and Vendor Questions Response State Hosted". This document cannot be a scanned document but must be an original. If the vendor elects to make the Security and Vendor Questions part of its response, the questions must be clearly indicated in the proposal's Table of Contents. A single numbering system must be used throughout the proposal.

1.2 PURPOSE OF REQUEST FOR PROPOSAL (RFP)

1.2.1 Background and Overview of Scope of Work:

The South Dakota Department of Corrections (DOC) website is due for a redesign. While navigation of the website, search-ability, content and continuity have been maintained, the time has come for an overhaul of doc.sd.gov to ensure customer expectations; connecting them with informational content that generates a meaningful and useful experience. Additionally, this overhaul includes rewriting the DOC intranet site – which is for internal staff use only.

The vendor will design, code, and populate a responsive internet and intranet website application. The vendor will work with DOC and the Bureau of Information and Telecommunications (BIT) to meet its technology and security requirements in all stages. In addition, they will design a new content management system (CMS) to populate all current and new content. The initial project plan is laid out in more detail below and in Section 3.0 of the Scope of Work, however, the State requests that the final contract be extended for three years after the final launch date with the option to renew the contract and an annual basis for up to three years after that.

1.3 ISSUING OFFICE AND RFP REFERENCE NUMBER

The South Dakota Department of Corrections is the issuing office for this document and all subsequent addenda relating to it, on behalf of the South Dakota Department of Corrections, Administration. The reference number for the transaction is 23RFP8586. This number must be referred to on all proposals, correspondence, and documentation relating to the RFP.

1.4 SCHEDULE OF ACTIVITIES

RFP Publication	April 12, 2023
Letter of Intent to Respond with Vendor Questions	May 15, 2023
Responses to Vendor Questions	May 29, 2023
Proposal Submission	**June 9 by 5:00 PM CST**
BIT Review	June 15, 2023
Award Decision/Contract Negotiation	July 6, 2023
Contract Start Date	July 21, 2023
Launch Date	October 6, 2023

1.5 SUBMITTING YOUR PROPOSAL

All proposals must be completed and received by June 9, 2023 by 5pm CST. Proposals received after the deadline will be ineligible for consideration.

1. An electronic PDF version must be emailed to Danna.Humig@state.sd.us
   - **Please place the following in the subject line:**
     DOC WEBSITE - 23RFP8586
2. If the file is too large to send via email, please provide an alternative option through an FTP site or DropBox with secured access. Please inform Danna Humig of this in an email with instructions on accessing.

Note: *No proposal shall be accepted from, or no contract or purchase order shall be awarded to any person, firm or corporation that is in arrears upon any obligations to the State of South Dakota, or that otherwise may be deemed irresponsible or unreliable by the State of South Dakota.*

1.6 CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION – LOWER TIER COVERED TRANSACTIONS

By signing and submitting this proposal, the offeror certifies that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation, by any Federal department or agency, from transactions involving the use of Federal funds. Where the offeror is unable to certify to any of the statements in this certification, the bidder shall attach an explanation to their offer.

1.7 NON-DISCRIMINATION STATEMENT

The State of South Dakota requires that all contractors, vendors, and suppliers doing business with any State agency, department, or institution, provide a statement of non-discrimination. By signing and submitting their proposal, the offeror certifies they do not discriminate in their employment practices with regard to race, color, creed, religion, age, sex, ancestry, national origin or disability.

1.8 MODIFICATION OR WITHDRAWAL OF PROPOSALS

Proposals may be modified or withdrawn by the offeror prior to the established due date and time. No oral, telephonic, telegraphic or facsimile responses or modifications to informal, formal bids, or Request for Proposals will be considered.

1.9 OFFEROR INQUIRIES

Only emailed questions will be accepted. All questions should be sent to: Danna.Humig@state.sd.us. Offeror may not rely on any other statements, either of a written or oral nature, that alter any specification or other term or condition of this RFP that have not originated from the DOC Point of Contact.

1.10 PROPRIETARY INFORMATION

The proposal of the successful offeror(s) becomes public information. Proprietary information can be protected under limited circumstances such as client lists and non-public financial statements. Pricing and service elements are not considered proprietary. An entire proposal may not be marked as proprietary. **Offerors must clearly identify in the Executive Summary and mark in the body of the proposal any specific proprietary information they are requesting to be protected. The Executive Summary must contain specific justification explaining why the information is to be protected.** Proposals may be reviewed and evaluated by any person at the discretion of the State. All materials submitted become the property of the State of South Dakota and may be returned only at the State's option.

1.11 LENGTH OF CONTRACT

The contract will begin July 21, 2023, or as mutually agreed upon by the two parties.

1. The launch date of both the Internet and Intranet must be no later than October 6, 2023.
2. The State requests that final contract terms be extended for three years after the final launch date with the option to renew the contract on an annual basis for up to three years after that.

1.12 RFP PROCESS

Any presentation or demonstration by an Offeror to clarify a proposal may be required at the sole discretion of the State. However, the State may award a contract based on the initial proposals received without a presentation or demonstration by the Offeror. If presentations and or demonstrations are required, they will be scheduled after the submission of proposals. Presentations and demonstrations will be made at the Offeror’s expense.

At the State’s discretion the Offeror may or may not be invited to have discussions with the State. The discussions can be before or after the RFP has been submitted. Discussions will be made at the Offeror’s expense.

This process is a Request for Proposal/Competitive Negotiation process. Each proposal shall be evaluated, and each respondent shall be available for negotiation meetings at the State’s request. The State reserves the right to negotiate on any and/or all components of every proposal submitted. From the time the proposals are submitted until the formal award of a contract, each proposal is considered a working document and as such, will be kept confidential. The negotiation discussions will also be held as confidential until such time as the award is completed.

2.0 STANDARD CONTRACT TERMS AND CONDITIONS. Any contract or agreement resulting from this RFP will include the State’s standard terms and conditions as listed below and the State’s standard I/T contract terms listed in Attachment A, along with any additional terms and conditions as negotiated by the parties:

2.1 The Contractor will perform those services described in the Scope of Work in Section 3.

2.2 The Contractor's services under this Agreement must launch on July 21, 2023, or as mutually agreed upon. The State requests that the final contract terms be extended for three years after the final launch date with the option to renew the contract and an annual basis for up to three years after that.

2.3 The Contractor will not use State equipment, supplies or facilities – unless otherwise discussed with the State for purposes such as the focus groups. The Contractor will provide the State with its Employer Identification Number, Federal Tax Identification Number or Social Security Number upon execution of this Agreement.

2.4 The State will make payment for services upon satisfactory completion of the services. The State will not pay Contractor's expenses as a separate item. Payment will be made pursuant to itemized invoices. Payment will be made consistent with SDCL chapter 5-26. Payment schedule based on project deliverables as outlined in the cost proposal and development of the project timeline of milestones.

2.5 The Contractor agrees to indemnify and hold the State of South Dakota, its officers, agents and employees, harmless from and against any and all actions, suits, damages, liability or other proceedings that may arise as the result of performing services hereunder. This section does not require the Contractor to be responsible for or defend against claims or damages arising solely from errors or omissions of the State, its officers, agents or employees.

2.6 The Contractor, at all times during the term of this Agreement, shall obtain and maintain in force insurance coverage of the types and with the limits as follows:

A. Commercial General Liability Insurance: The Contractor shall maintain occurrence based commercial general liability insurance or equivalent form with a limit of not less than $1,000,000.00 for each occurrence. If such insurance contains a general aggregate limit it shall apply separately to this Agreement or be no less than two times the occurrence limit.

B. Professional Liability Insurance or Miscellaneous Professional Liability Insurance: The Contractor agrees to procure and maintain professional liability insurance or miscellaneous professional liability insurance with a limit not less than $1,000,000.00.

C. Business Automobile Liability Insurance: The Contractor shall maintain business automobile liability insurance or equivalent form with a limit of not less than $1,000,000.00 for each accident. Such insurance shall include coverage for owned, hired and non-owned vehicles.

D. Worker's Compensation Insurance: The Contractor shall procure and maintain workers' compensation and employers' liability insurance as required by SD law.

Before beginning work under this Agreement, Contractor shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement. In the event a substantial change in insurance, issuance of a new policy, cancellation or nonrenewal of the policy, the Contractor agrees to provide immediate notice to the State and provide a new certificate of insurance showing continuous coverage in the amounts required. Contractor shall furnish copies of insurance policies if requested by the State.

2.7 While performing services hereunder, the Contractor is an independent contractor and not an officer, agent, or employee of the State of South Dakota.

2.8 Contractor agrees to report to the State any event encountered in the course of performance of this Agreement which results in injury to the person or property of third parties, or which may otherwise subject Contractor or the State to liability. Contractor shall report any such event to the State immediately upon discovery.

Contractor's obligation under this section shall only be to report the occurrence of any event to the State and to make any other report provided for by their duties or applicable law. Contractor's obligation to report shall not require disclosure of any information subject to privilege or confidentiality under law (e.g., attorney-client communications). Reporting to the State under this section shall not excuse or satisfy any obligation of Contractor to report any event to law enforcement or other entities under the requirements of any applicable law.

2.9 This Agreement may be terminated by either party hereto upon thirty (30) days written notice. In the event the Contractor breaches any of the terms or conditions hereof, this Agreement may be terminated by the State at any time with or without notice. If termination for such a default is effected by the State, any payments due to Contractor at the time of termination may be adjusted to cover any additional costs to the State because of Contractor's default. Upon termination the State may take over the work and may award another party an agreement to complete the work under this Agreement. If after the State terminates for a default by Contractor it is determined that Contractor was not at fault, then the Contractor shall be paid for eligible services rendered and expenses incurred up to the date of termination.

2.10 This Agreement depends upon the continued availability of appropriated funds and expenditure authority from the Legislature for this purpose. If for any reason the Legislature fails to appropriate funds or grant expenditure authority, or funds become unavailable by operation of law or federal funds reductions, this Agreement will be terminated by the State. Termination for any of these reasons is not a default by the State nor does it give rise to a claim against the state.

2.11 This Agreement may not be assigned without the express prior written consent of the State. This Agreement may not be amended except in writing, which writing shall be expressly identified as a part hereof, and be signed by an authorized representative of each of the parties hereto.

2.12 This Agreement shall be governed by and construed in accordance with the laws of the State of South Dakota. Any lawsuit pertaining to or affecting this Agreement shall be venued in Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota.

2.13 The Contractor will comply with all federal, state and local laws, regulations, ordinances, guidelines, permits and requirements applicable to providing services pursuant to this Agreement, and will be solely responsible for obtaining current information on such requirements.

2.14 If the vendor chooses to subcontract any one part of the components listed in section 3.1 to complete the requirements of this RFP, DOC must be notified and reserves the right to veto. The Contractor will include provisions in its subcontracts requiring its subcontractors to comply with the applicable provisions of this Agreement, to indemnify the State, and to provide insurance coverage for the benefit of the State in a manner consistent with this Agreement. The Contractor will cause its subcontractors, agents, and employees to comply, with applicable federal, state and local laws, regulations, ordinances, guidelines, permits and requirements will adopt such review and inspection procedures as are necessary to assure such compliance.

2.15 Contractor hereby acknowledges and agrees that all reports, plans, specifications, technical data, miscellaneous drawings, software system programs and documentation, procedures, or files, operating instructions and procedures, source code(s) and documentation, including those necessary to upgrade and maintain the software program, and all information contained therein provided to the State by the Contractor in connection with its performance of services under this Agreement shall belong to and is the property of the State and will not be used in any way by the Contractor without the written consent of the State. Papers, reports, forms, software programs, source code(s) and other material which are a part of the work under this Agreement will not be copyrighted without written approval of the State.

2.16 The Contractor certifies that neither Contractor nor its principals are presently debarred, suspended, proposed for debarment or suspension, or declared ineligible from participating in transactions by the federal government or any state or local government department or agency. Contractor further agrees that it will immediately notify the State if during the term of this Agreement Contractor or its principals become subject to debarment, suspension or ineligibility from participating in transactions by the federal government, or by any state or local government department or agency.

2.17 Any notice or other communication required under this Agreement shall be in writing and sent to the address set forth above. Notices or communications to or between the parties shall be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination shall be sent by registered or certified mail, or, if personally delivered, when received by such party.

2.18 In the event that any court of competent jurisdiction shall hold any provision of this Agreement unenforceable or invalid, such holding shall not invalidate or render unenforceable any other provision hereof.

2.19 All other prior discussions, communications and representations concerning the subject matter of this Agreement are superseded by the terms of this Agreement, and except as specifically provided herein, this Agreement constitutes the entire agreement with respect to the subject matter hereof.

2.20 For contractors, vendors, suppliers, or subcontractors with five (5) or more employees who enter into a contract with the State of South Dakota that involves the expenditure of one hundred thousand dollars ($100,000) or more, by submitting a response to this solicitation or agreeing to contract with the State, the bidder or offeror certifies and agrees that the following information is correct:

The bidder or offeror, in preparing its response or offer or in considering proposals submitted from qualified, potential vendors, suppliers, and subcontractors, or in the solicitation, selection, or commercial treatment of any vendor, supplier, or subcontractor, has not refused to transact business activities, has not terminated business activities, and has not taken other similar actions intended to limit its commercial relations, related to the subject matter of the bid or offer, with a person or entity on the basis of Israeli national origin, or residence or incorporation in Israel or its territories, with the specific intent to accomplish a boycott or divestment of Israel in a discriminatory manner. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to reject the bid or response submitted by the bidder or offeror on this project and terminate any contract awarded based on the bid or response. The successful bidder or offeror further agrees to provide immediate written notice to the contracting executive branch agency if during the term of the contract it no longer complies with this certification and agrees such noncompliance may be grounds for contract termination.

2.21 In preparing its response or offer or in considering proposals submitted from qualified, potential vendors, suppliers, and subcontractors, or in the solicitation, selection, or commercial treatment of any vendor, supplier, or subcontractor, Contractor is not an entity, regardless of its principal place of business, that is ultimately owned or controlled, directly or indirectly, by a foreign national, a foreign parent entity, or foreign government from China, Iran, North Korea, Russia, Cuba, or Venezuela, as defined by South Dakota Executive Order 2023-02.

Contractor further agrees that, if this certification is false, such false certification will constitute grounds for the State to terminate this Agreement. Contractor further agrees to provide immediate written notice to the State if during the term of this Agreement it no longer complies with this certification and agrees such noncompliance may be grounds for termination of this Agreement.

3.0 SCOPE OF WORK

The vendor will design, code, and populate a responsive internet and intranet website application. The vendor will work with DOC to meet its technology and security requirements in all stages. In addition, they will design a new content management system (CMS) to populate all current and new content.

Proposals must reference all components listed below and in the Scope of Work to be included in the selection review process. If the vendor chooses to subcontract any one part of the key components listed below to complete the requirements of this RFP, DOC must be notified and reserves the right to veto. (See additional language in 2.14.)

3.1 Project components:

1. Website design, testing, and execution (includes Internet and Intranet sites).
2. User and security testing and feedback integration.
3. Maintenance agreement and future recommendations.
4. Project management role to be completed by the vendor.
5. Photo library of new images to choose from for website layout and design.
6. Responsive design to render on any handheld or tablet device.
7. Development, testing and implementation of the DOC Intranet website.
8. Landing page for correctional industries business/online ordering.
9. Payment option for outstanding bills.
10. Offender locator which needs to interface with Syscon offender management system.

3.2 Key Website Features:

1. Search engine functionality must be modernized and set to the highest standard of excellence to offer an enhanced customer experience.
2. Content management system programming and implementation.

3. Enhanced newsroom/press release archive.
4. Staff directory/contact page consolidated through and features first and second tier leadership profiles.
5. Ability to focus in on key audience types who will visit and navigate the site (example: family member, parolee, victim, etc.).
6. Live data and graphics through Power BI or similar program.
7. Utilization of fillable forms on the website and Intranet.
8. Incorporate DOC policies on intranet in user-friendly format.

3.3 Additional Areas of Work

1. Vendor meetings – TBD – and coordinated by the vendor project manager.
    a. Includes face to face and virtual meetings as agreed upon by the DOC and the vendor.
    b. Weekly meetings throughout the length of the project between the DOC workgroup and vendor project manager.
    c. These meetings will include status updates, percent of project complete, issues impacting target completion date and action items.
2. Internal DOC workgroup will co-lead the content development with insight and feedback from the vendor.
3. The DOC workgroup will work collectively with the vendor to ensure written content fits the program scope, action and audience appropriately.
4. Outline project management milestones.
    a. Identify when test sessions will occur during major components of development along with all other details associated with the major components listed in the previous section.
5. Identify and share other creative enhancements and opportunities for the Department to embark on during this development process.
6. Quarterly report on website usage and performance.
7. Explain your recommendation for hosting on State of South Dakota servers vs. vendor-hosted servers.
8. Security scans and assessments (see 3.9 for more details on IT requirements) conducted prior to launch date.
    a. What this means is that we will need the website near completion (90-95 percent complete) by September 22, 2023. Launch date no later than October 6, 2023.

3.4 Goals

1. Begin work in July 2023 with a comprehensive timeline and project management outline associate with the scope of work.
2. Develop a maintenance agreement.
3. Design and share a minimum of three mock website templates (include secondary page designs) for the new doc.sd.gov and similar Intranet style.
4. Code and construct the new doc.sd.gov.
5. Code and construct the new doc.sd.gov Intranet site.
6. Assist with content creation and page development of doc.sd.gov.

- DOC will provide a comprehensive review of content we wish to carry over from current website to new website.
- Help support imagery, design and layout of all pages of the site.

7. Prepare a style guide for doc.sd.gov.

8. Facilitate user testing in partnership with DOC.
9. Work with DOC and the state's IT agency to successfully launch the new doc.sd.gov.

3.5 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.

3.6 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. SSO is required to login and to enter the CMS application and to perform updates and routine edits to the Internet and Intranet websites.

The SSO supports two industry-standard protocols: OpenID Connect and OAuth 2.0 (preferred). This identity management will handle password recovery. Multi-factor Authentication (MFA) is required for all application Administrators and may be required for other users.

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

3.7 Interfaces and Integration

The vendor must describe how the system can adapt to business necessary interfaces using widely adopted open APIs and standards. Additionally, Department of Corrections expects that the vendor 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 shall be included in the proposal.

3.8 Project Deliverables/Approach/Methodology

If the State will be hosting the solution the vendor 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 vendor elects to make the diagram part of the proposal, then the location of the diagram must be clearly indicated in the Table of Contents.

3.9 For state-hosted systems that reside in a state-managed cloud:

To minimize impacts to project schedules, vendors are required to provide architectural plans, resource needs, permission plans, and all interfaces – both internal to the state and internet facing for cloud hosted systems. The documentation provided will be reviewed as part of the initial assessment process. If selected for award of a contract, and once the state has approved the submitted materials, a test environment will be provided after contract signature. Systems will be reviewed again before being moved to a production environment. Any usage or processes that are deemed out of compliance with what was approved or represent excessive consumption or risk will require remediation before being moved to production.

If the vendor 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 vendor 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 vendor should state whether its proposed solution will operate in a virtualized environment. Vendor 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 vendor hosted solution.

> *Application must be developed in the Microsoft Technology Stack (Asp.net, Razor, MVC, etc). The CMS recommended is Umbraco, for any other CMS to be considered, they must be within the Microsoft Technology Stack. Database (for the data repository) must be MS SQL or MS compliant database.*

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

The vendor 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 vendor. Any licensing costs for the test system must be included with the costs.

At BIT's discretion, any code changes made by the vendor, 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 vendor. 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 vendor 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 vendor will, unless approved otherwise by BIT, diagnosis the problem and make all fixes on the test system. The vendor is expected to provide proof, to BIT, of the actions taken to remediate the problem that lead 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 vendor if the vendor feels that revealing the fix will put the vendor's intellectual property at risk.

All solutions acquired by the State that are hosted by the vendor, including Software as a Service, or hosted by a third-party for the vendor will be subjected to security scans by BIT or preapproved detailed security scan report provided by the vendor. The scan report sent in with the proposal can be redacted by the vendor. 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 vendor 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 vendor'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:

1. The system that was evaluated (URL if possible, but mask it if needed).
2. The categories that were evaluated (example: SQL injection, cross site scripting, etc.)
3. What were the general findings, (meaning how many SQL injection issues were found, what was the count per category)
4. 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 vendor or the vendor's costs associated with the State's scans must be part of the vendor's bid. If the vendor 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 vendor was to do the security scan.

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 vendor 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 vendor that generates email cannot use "@state.sd.us" as the originating domain name per state security policy.

As part of this project, the vendor 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 vendor 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 vendor 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 vendor 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 vendor's proposal must indicate this and give the reason why the data cannot be sanitized as per the methods in NIST 800-88.

The vendor's solution cannot include any hardware or hardware components manufactured by Huawei Technologies Company or ZTE Corporation or any subsidiary or affiliate of such entities. This includes hardware going on the State's network as well as the vendor's network if the vendor'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 vendor's solution requires accounts allowing access to State systems, then the vendor must indicate the number of the vendor'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 vendor 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 vendor 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 will be deleted after Y days if it is not used.

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. A vendor **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.

4.0 RESOURCES AND STATE ORGANIZATIONAL STRUCTURE

The Bureau of Information and Telecommunications (BIT) is the state organization that provides IT services for the state and will be part of the testing and security scans along with their own information technology review. However, will not play a role in routine development, creative process, or regular meetings between the State and the selected vendor.

4.1. DOC Team Organization:

- DOC Division Director of Finance & Administration –Brittni Skipper
- DOC Public Information Officer – Michael Winder – main POC with vendor project manager
- DOC Team Members
    - Michael Winder – content specialist, web manager, information officer, digital strategist
    - Bridget Coppersmith – data & planning analysis associate director, grants manager
    - Justin Winters – correctional industries manager
    - Danna Humig – contract compliance/RFP POC, business operations associate director
    - Nicole Gednalske – constituent services
    - Joy Ellefson – data systems manager
- DOC Internal Workgroup – TBD - program area experts, content creators and reviewers

5.0 FORMAT OF SUBMISSION

All proposals should be prepared simply and provide a direct, concise explanation of the Offeror's proposal and qualifications. Offerors are required to provide an electronic copy of their response as previously mentioned. The offeror is cautioned that it is the offeror's sole responsibility to submit information related to the evaluation categories and that the State of South Dakota is under no obligation to solicit such information if it is not included with the proposal. The offeror's failure to submit such information may cause an adverse impact on the evaluation of the proposal. Offerors and their agents (including subcontractors, employees, consultants, or anyone else acting on their behalf) must direct all of their questions or comments regarding the RFP, the evaluation, etc. to Danna Humig. Inappropriate contacts are grounds for suspension and/or exclusion from specific procurements. Offerors and their agents who have questions regarding this matter should contact Danna.Humig@state.sd.us.

The offeror may be required to submit a copy of their most recent audited financial statements upon the State's request. The proposal should be page numbered and should have an index and/or a table of contents referencing the appropriate page number.

Proposals should be prepared using the order of the following headings.

1. Understanding of Project
2. Deliverables/Goals
4. Project Plan and Detailed Timeline

5. Project Team Organizational Structure and Experience
    a. Identify who will be the project manager working to ensure all deliverables of the contract are met.
6. Overall Project Cost Proposal
    a. Outline each component as a line item to indicate the cost of each.
    b. Note that cost will be considered as a factor in the decision-making process.

6.0 UNDERSTANDING OF PROJECT

To demonstrate your comprehension of the project, please summarize your understanding of what the work is and what the work will entail. This should include, but not be limited to your understanding of the purpose and scope of the project, critical success factors and potential problems related to the project and your understanding of the deliverables. Your specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements should be included.

7.0 CORPORATE QUALIFICATIONS

Please provide responses to the each of the following questions in your proposal.

A. What year was your parent company (if applicable) established?
B. What is the business of your parent company?
C. What is the total number of employees in the parent company?
D. What are the total revenues of your parent company?
E. How many employees of your parent company have the skill set to support this effort?
F. How many of those employees are accessible to your organization for active support?
G. What year was your firm established?
H. Has your firm ever done business under a different name and if so what was the name?
I. How many employees does your firm have?
J. How many employees in your firm are involved in this type of project?
K. How many of those employees are involved in on-site project work?
L. What percent of your parent company’s revenue (if applicable), is produced by your firm?
M. Corporate resources available to perform the work, including any specialized services, within the specified time limits for the project
N. Availability to the project locale
O. Familiarity with the project locale
P. Has your firm ever done business with other governmental agencies? If so, please provide references.
Q. Has your firm ever done business with the State of South Dakota? If so, please provide references.
R. Has your firm ever done projects that are like or similar to this project? If so, how many clients are using your solution? Please provide a list of four or more locations of the same approximant nature as the State where your application is in use along with contact names and numbers for those sites.
S. Provide third party security audits of the four projects you provided for R above (if applicable). The State will sign a non-disclosure statement, as needed, to receive these audits, within the limits of the State’s open records law. If there are no audits of these projects then provide, unedited and un-redacted results of such security testing/scanning from third-party companies and/or tools that has been run within the past 90 days. To protect proprietary or confidential information, the state will agree to non-disclosure of any information provided as a result of such a request as appropriate.

8.0 PROJECT PLAN AND TIMELINE

Provide a project plan that indicates how you will complete the required scope of work and project requirements and deliverables as outlined in section 3.0. See DOC proposed timeline and high-level expectations.

1. Proposed project management techniques and project manager identified
2. Number of Vendor staff needed
3. Tasks to be performed (within phase as applicable)
4. Deliverables created by each task
5. Dates by which each task will be completed
6. Resources assigned to each task
7. Required state agency support
8. Show task dependencies
9. Training (if applicable)

9.0 COST PROPOSAL

Include a cost proposal as part of the RFP submission. Please also note that cost will be considered as a factor in the decision-making process.

10.0 PROPOSAL EVALUATION AND AWARD PROCESS

After determining that a proposal satisfies the mandatory requirements stated in the Request for Proposal, the evaluator(s) shall use subjective judgment in conducting a comparative assessment of the proposal by considering each of the following criteria:

- Specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements;
- Resources available to perform the work, including any specialized services, within the specified time limits for the project;
- Record of past performance, including price and cost data from previous projects, quality of work, ability to meet schedules, cost control, and contract administration;
- Availability and familiarity of project locale;
- Proposed project management techniques;
- Ability and proven history in handling special project constraints;
- Experience and reliability of the offeror's organization are considered subjectively in the evaluation process;
- The qualifications of the personnel proposed by the offeror to perform requirements of RFP;
- The State reserves the right to reject any or all proposals, waive technicalities, and make award(s) as deemed to be in the best interest of the State of South Dakota;
- The requesting agency and the highest ranked offeror shall mutually discuss and refine the scope of services for the project and shall negotiate terms, including compensation and performance schedule;
- If the agency and the highest ranked offeror are unable for any reason to negotiate a contract at a compensation level that is reasonable and fair to the agency, the agency shall, either orally or in writing, terminate negotiations with the contractor. The agency may then negotiate with the next highest ranked contractor; and
- The negotiation process may continue through successive offerors, according to agency ranking, until an agreement is reached, or the agency terminates the contracting process.

11.0 NON-STANDARD HARDARE 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 9.0 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.

12.0 BEST AND FINAL OFFERS

The State reserves the right to request best and final offers. If so, the State will initiate the request for best and final offers; best and final offers may not be initiated by a Vendor. Best and final offers may not be necessary if the State is satisfied with proposals received. If best and final offers are sought, the State will document which Vendors will be notified and provide them opportunity to submit best and final offers. Requests for best and final offers will be sent stating any specific areas to be covered and the date and time in which the best and final offer must be returned. Conditions, terms, or price of the proposal may be altered or otherwise changed, provided the changes are within the scope of the request for proposals and instructions contained in the request for best and final offer. If a Vendor does not submit a best and final offer or a notice of withdrawal, the Vendor's previous proposal will be considered as the Vendor's best and final proposal. After best and final offers are received, final evaluations will be done.

Attachment A
Bureau of Information and Telecommunications
Required IT Contract Terms

Any contract resulting from this RFP will include the State's required IT terms and conditions as listed below, along with any additional terms and conditions as negotiated by the parties. Due to the changing landscape of IT security and data privacy, the State reserves the right to add additional IT terms and conditions or modify the IT terms and conditions listed below to the resulting contract:

Pursuant to South Dakota Codified Law § 1-33-44, the Bureau of Information and Telecommunications ("BIT") oversees the acquisition of office systems technology, software, and services; telecommunication equipment, software, and services; and data processing equipment, software, and services for departments, agencies, commissions, institutions, and other units of state government. As part of its duties as the Executive Branch's centralized IT agency, BIT requires the contract terms and conditions of this Exhibit XX. For purposes of this Exhibit, [Vendor Name] will be referred to as the "Vendor."

It is understood and agreed to by all parties that BIT has reviewed and approved only this Exhibit. Due to the ever-changing security and regulatory landscape in IT and data privacy, before renewal of this Agreement BIT must review and approve the clauses found in this Exhibit as being the then current version of the clauses and if any additional required clauses are needed. Changes to clauses in this Exhibit must be approved in writing by all parties before they go into effect and a renewal of this Agreement is possible.

The Parties agree, when used in this Exhibit, the term "Vendor" will mean the Vendor and the Vendor's employees, subcontractors, agents, assigns, and affiliated entities.

Section I. Confidentiality of Information

For purposes of this paragraph, "State Proprietary Information" will include all information disclosed to the Vendor by the State. The Vendor will not disclose any State Proprietary Information to any third person for any reason without the express written permission of a State officer or employee with authority to authorize the disclosure. The Vendor must not: (i) disclose any State Proprietary Information to any third person unless otherwise specifically allowed under this Agreement; (ii) make any use of State Proprietary Information except to exercise rights and perform obligations under this Agreement; (iii) make State Proprietary Information available to any of its employees, officers, agents, or third party consultants except those who have a need to access such information and who have agreed to obligations of confidentiality at least as strict as those set out in this Agreement. The Vendor is held to the same standard of care in guarding State Proprietary Information as it applies to its own confidential or proprietary information and materials of a similar nature, and no less than holding State Proprietary Information in the strictest confidence. The Vendor must protect the confidentiality of the State's information from the time of receipt to the time that such information is either returned to the State or destroyed to the extent that it cannot be recalled or reproduced. The Vendor agrees to return all information received from the State to the State's custody upon the end of the term of this Agreement, unless otherwise agreed in a writing signed by both parties. State Proprietary Information will not include information that:

A. was in the public domain at the time it was disclosed to the Vendor,
B. was known to the Vendor without restriction at the time of disclosure from the State,
C. that was disclosed with the prior written approval of State's officers or employees having authority to disclose such information,
D. was independently developed by the Vendor without the benefit or influence of the State's information, and
E. becomes known to the Vendor without restriction from a source not connected to the State of South Dakota.

State's Proprietary Information can include names, social security numbers, employer numbers, addresses and other data about applicants, employers or other clients to whom the State provides services of any kind. The Vendor understands that this information is confidential and protected under State law. The Parties mutually agree that neither of them nor any subcontractors, agents, assigns, or affiliated entities will disclose the contents of this Agreement except as required by applicable law or as necessary to carry out the terms of the Agreement or to enforce that Party's rights under this Agreement. The Vendor acknowledges that the State and its agencies are public entities and thus may be bound by South Dakota open meetings and open records laws. It is therefore not a breach of this Agreement for the State to take any action that the State reasonably believes is necessary to comply with South Dakota open records or open meetings laws.

Section II. Cyber Liability Insurance

The Vendor will maintain cyber liability insurance with liability limits in the amount of $3,000,000 to protect any and all State data the Vendor receives as part of the project covered by this agreement including State data that may reside on devices, including laptops and smart phones, utilized by Vendor employees, whether the device is owned by the employee or the Vendor. If the Vendor has a contract with a third-party to host any State data the Vendor receives as part of the project under this Agreement, then the Vendor will include a requirement for cyber liability insurance as part of the contract between the Vendor and the third-party hosting the data in question. The third-party cyber liability insurance coverage will include State Data that resides on devices, including laptops and smart phones, utilized by third-party employees, whether the device is owned by the employee or the third-party Vendor. The cyber liability insurance will cover expenses related to the management of a data breach incident, the investigation, recovery and restoration of lost data, data subject notification, call management, credit checking for data subjects, legal costs, and regulatory fines. Before beginning work under this Agreement, the Vendor will furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement and which provide that such insurance may not be canceled, except on 30 days prior written notice to the State. The Vendor will furnish copies of insurance policies if requested by the State. The insurance will stay in effect for three years after the work covered by this Agreement is completed.

Section III. Rejection or Ejection of Vendor

The State, at its option, may require the vetting of any of the Vendor, and the Vendor's subcontractors, agents, Assigns, or affiliated entities. The Vendor is required to assist in this process as needed.

The State reserves the right to reject any person from participating in the project or require the Vendor to remove from the project any person the State believes is detrimental to the project or is considered by the State to be a security risk. The State will provide the Vendor with notice of its determination, and the reasons for the rejection or removal if requested by the Vendor. If the State signifies that a potential security violation exists with respect to the request, the Vendor must immediately remove the individual from the project.

Section IV. Domain Name Ownership

Any website(s) that the Vendor creates as part of this Agreement must have the domain name registered by and owned by the State. If, as part of this Agreement, the Vendor is providing a service that utilizes a website with the domain name owned by the Vendor, the Vendor must give 30 days' written notice before abandoning the site. If the Vendor intends to sell the site to another party, the Vendor must give the State 30 days' written notice and grant the State the right of first refusal. For any site or domain, whether hosted by the Vendor or within the State web infrastructure, any and all new web content should first be created in a development environment and then subjected to security scan before being approved for a move up to the production level. This paragraph does not include websites developed for the Vendor's internal use.

Section V. Non-Disclosure and Separation of Duties

The Vendor will enforce separation of job duties and require non-disclosure agreements of all staff that have or can have access to State Data or the hardware that State Data resides on. The Vendor will limit staff knowledge to those staff who duties that require them to have access to the State Data or the hardware the State Data resides on.

Section VI. Cessation of Business

The Vendor will notify the State of impending cessation of its business or that of a tiered provider and the Vendor's contingency plan. This plan should include the immediate transfer of any previously escrowed assets and data and State access to the Vendor's facilities to remove or destroy any state-owned assets and data. The Vendor will implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the State. The Vendor will provide a fully documented service description and perform and document a gap analysis by examining any differences between its services and those to be provided by its successor. The Vendor will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the State. The Vendor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and impact on the State, all such work to be coordinated and performed in advance of the formal, final transition date.

Section VII. Legal Requests for Data

Except as otherwise expressly prohibited by law, the Vendor will:

A. Immediately notify the State of any subpoenas, warrants, or other legal orders, demands or requests received by the Vendor seeking State Data maintained by the Vendor,
B. Consult with the State regarding the Vendor's response,
C. Cooperate with the State's requests in connection with efforts by the State to intervene and quash or modify the legal order, demand or request, and
D. Upon the State's request, provide the State with a copy of both the demand or request and its proposed or actual response.

Section VIII. eDiscovery

The Vendor will contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to State Data. The Vendor will not respond to service of process, and other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

Section IX. Audit Requirements

The Vendor warrants and agrees it is aware of and complies with all audit requirements relating to the classification of State Data the Vendor stores, processes, and accesses. Depending on the data classification, this may require the Vendor to grant physical access to the data hosting facilities to the State or a federal agency. The Vendor will notify the State of any request for physical access to a facility that hosts or processes State Data by any entity other than the State.

Section X. Annual Risk Assessment

The Vendor will conduct an annual risk assessment or when there has been a significant system change. The Vendor will provide verification to the State's contact upon request that the risk assessment as taken place. At a minimum, the risk assessment will include a review of the:

A. Penetration testing of the Vendor's system;
B. Security policies and procedures;
C. Disaster recovery plan;
D. Business Associate Agreements; and
E. Inventory of physical systems, devices, and media that store or utilize ePHI for completeness.

If the risk assessment provides evidence of deficiencies, a risk management plan will be produced. Upon request by the State, the Vendor will send a summary of the risk management plan to the State's contact. The summary will include completion dates for the risk management plan's milestones. Upon request by the State, the Vendor will send updates on the risk management plan to the State's contact. Compliance with this Section may be met if the Vendor provides proof to the State that the Vendor is FedRAMP Certified and has maintained FedRAMP Certification.

Section XI. Independent Audit

The Vendor will disclose any independent audits that are performed on any of the Vendor's systems tied to storing, accessing, and processing State Data. This information on an independent audit(s) must be provided to the State in any event, whether the audit or certification process is successfully completed or not. The Vendor will provide a copy of the findings of the audit(s) to the State. Compliance with this Section may be met if the Vendor provides a copy of the Vendor's SOC 2 Type II report to the State upon request.

Section XII. Service Level Agreements

The Vendor warrants and agrees that the Vendor has provided to the State all Service Level Agreements (SLA) related to the deliverables of the Agreement. The Vendor further warrants that it will provide the deliverables to the State in compliance with the SLAs.

Section XIII. Access Attempts

The Vendor will log all access attempts, whether failed or successful, to any system connected to the hosted system which can access, read, alter, intercept, or otherwise impact the hosted system or its data or data integrity. For all systems, the log must include at least: login page used, username used, time and date stamp, incoming IP for each authentication attempt, and the authentication status, whether successful or not. Logs must be maintained not less than 7 years in a searchable database in an electronic format that is un-modifiable. At the request of the State, the Vendor agrees to grant the State access to those logs to demonstrate compliance with the terms of this Agreement and all audit requirements related to the hosted system.

Section XIV. Access to State Data

Unless this Agreement is terminated, the State's access to State Data amassed pursuant to this Agreement will not be hindered if there is a:

A. Contract dispute between the parties to this Agreement,
B. There is a billing dispute between the parties to this Agreement, or
C. The Vendor merges with or is acquired by another company.

Section XV. Password Protection

All aspects of the Vendor's products provided to the State pursuant to this Agreement will be password protected. If the Vendor provides the user with a preset or default password, that password cannot include any Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI), or any information defined under federal or state law, rules, or regulations as confidential information or fragment thereof. On an annual basis, the Vendor will document its password policies for all Vendor employees to ensure adequate password protections are in place. The process used to reset a password must include security questions or Multifactor Authentication. Upon request, the Vendor will provide to the State the Vendor's password policies, logs, or administrative settings to demonstrate the password policies are actively enforced.

Section XVI. Provision of Data

State Data is any data produced or provided by the State as well as any data produced or provided for the State by the Vendor or a third-party.

Upon notice of termination by either party or upon reaching the end of the term of this Agreement, the Vendor will provide the State all current State Data in a non-proprietary format. In addition, the Vendor agrees to extract any information (such as metadata, which includes data structure descriptions, data dictionary, and data) stored in repositories not hosted on the State's IT infrastructure in a format chosen by the State. If the State's chosen format is not possible, the Vendor will extract the information into a text file format and provide it to the State.

Upon the effective date of the termination of this Agreement, the Vendor will again provide the State with all current State Data in a non-proprietary format. In addition, the Vendor will again extract any information (such as metadata) stored in repositories not hosted on the State's IT infrastructure in a format chosen by the State. As before, if the State's chosen format is not possible, the Vendor will extract the information into a text file format and provide it to the State.

Section XVII. Threat Notification

A credible security threat consists of the discovery of an exploit that a person considered an expert on Information Technology security believes could be used to breach any aspect of a system that is holding State Data or a product provided by the Vendor. Upon becoming aware of a credible security threat with the Vendor's product(s) and or service(s) being used by the State, the Vendor or any subcontractor supplying product(s) or service(s) to the Vendor needed to fulfill the terms of this Agreement will notify the State within two business days of any such threat. If the State requests, the Vendor will provide the State with information on the threat.

Section XVIII. Security Incident Notification for Non-Health Information

The Vendor will implement, maintain, and update Security Incident procedures that comply with all State standards and Federal and State requirements. A Security Incident is a violation of any BIT security or privacy policies or contract agreements involving sensitive information, or the imminent threat of a violation. The BIT security policies can be found in the Information Technology Security Policy ("ITSP") attached as Exhibit _____. The State requires notification of a Security Incident involving any of the State's sensitive data in the Vendor's possession. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party. The parties agree that, to the extent probes and reconnaissance scans common to the industry constitute Security Incidents, this Agreement constitutes notice by the Vendor of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State will be required. Probes and scans include, without limitation, pings and other broadcast attacks in the Vendor's firewall, port scans, and unsuccessful log-on attempts, if such probes and reconnaissance scans do not result in a Security Incident as defined above. Except as required by other legal requirements the Vendor will only provide notice of the incident to the State. The State will determine if notification to the public will be by the State or by the Vendor. The method and content of the notification of the affected parties will be coordinated with, and is subject to approval by the State, unless required otherwise by legal requirements. If the State decides that the Vendor will be distributing, broadcasting to or otherwise releasing information on the Security Incident to the news media, the State will decide to whom the information will be sent, and the State must approve the content of any information on the Security Incident before it may be distributed, broadcast, or otherwise released. The Vendor must reimburse the State for any costs associated with the notification, distributing, broadcasting, or otherwise releasing information on the Security Incident.

A. The Vendor must notify the State contact within 12 hours of the Vendor becoming aware that a Security Incident has occurred. If notification of a Security Incident to the State contact is delayed because it may impede a criminal investigation or jeopardize homeland or federal security, notification must be given to the State within 12 hours after law-enforcement provides permission for the release of information on the Security Incident.

B. Notification of a Security Incident at a minimum is to consist of the nature of the data exposed, the time the incident occurred, and a general description of the circumstances of the incident. If all of the information is not available for the notification within the specified time period, the Vendor must provide the State with all of the available information along with the reason for the incomplete notification. A delay in excess of 12 hours is acceptable only if it is necessitated by other legal requirements.

C. At the State's discretion within 12 hours the Vendor must provide to the State all data available including:

1. name of and contact information for the Vendor's Point of Contact for the Security Incident,
2. date and time of the Security Incident,
3. date and time the Security Incident was discovered,
4. description of the Security Incident including the data involved, being as specific as possible,
5. the potential number of records, and if unknown the range of records,
6. address where the Security Incident occurred, and
7. the nature of the technologies involved. If not all of the information is available for the notification within the specified time period, the Vendor must provide the State with all of the available information along with the reason for the incomplete information. A delay in excess of 12 hours is acceptable only if it is necessitated by other legal requirements.

D. If the Security Incident falls within the scope of South Dakota Codified Law Chapter 22-40, the Vendor is required to comply with South Dakota law.

The requirements of subsection D of this Section do not replace the requirements of subsections A, B, and C, but are in addition to them.

Section XIX. Handling of Security Incident for Non-Health Information

At the State's discretion, the Vendor will preserve all evidence regarding a security incident including but not limited to communications, documents, and logs. The Vendor will also:

A. fully investigate the incident,
B. cooperate fully with the State's investigation of, analysis of, and response to the incident,
C. make a best effort to implement necessary remedial measures as soon as it is possible, and
D. document responsive actions taken related to the Security Incident, including any post-incident review of events and actions taken to implement changes in business practices in providing the services covered by this Agreement.

If, at the State's discretion the Security Incident was due to the actions or inactions of the Vendor and at the Vendor's expense the Vendor will use a credit monitoring service, call center, forensics company, advisors, or public relations firm whose services are acceptable to the State. At the State's discretion the Vendor will offer two years of credit monitoring to each person whose data was compromised. The State will set the scope of any investigation. The State reserves the right to require the Vendor undergo a risk assessment where the State will determine the methodology and scope of the assessment and who will perform the assessment (a third-party vendor may be used). Any risk assessment required by this Section will be at the Vendor's expense.

If the Vendor is required by federal law or regulation to conduct a Security Incident or data breach investigation, the results of the investigation must be reported to the State within 12 hours of the investigation report being completed. If the Vendor is required by federal law or regulation to notify the affected parties, the State must also be notified, unless otherwise required by law.

Notwithstanding any other provision of this Agreement, and in addition to any other remedies available to the State under law or equity, the Vendor will reimburse the State in full for all costs incurred by the State in investigation and remediation of the Security Incident including, but not limited, to providing notification to regulatory agencies or other entities as required by law or contract. The Vendor will also pay all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident.

Section XX. Adverse Event

The Vendor must notify the State contact within three days if the Vendor becomes aware that an Adverse Event has occurred. An Adverse Event is the unauthorized use of system privileges, unauthorized access to State Data, execution of malware, physical intrusions and electronic intrusions that may include network, applications, servers, workstations, and social engineering of staff. If the Adverse Event was the result of the Vendor's actions or inactions, the State can require a risk assessment of the Vendor the State mandating the methodology to be used as well as the scope. At the State's discretion a risk assessment may be performed by a third party at the Vendor's expense. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party.

Section XXI. Source Code

The Vendor will provide to the South Dakota Bureau of Information and Telecommunications, for safekeeping, a copy of source code developed or maintained for use by the State under the terms of this Agreement. The source code provided will be the version currently running on the State's production environment.

Section XXII. Browser

The system, site, or application must be compatible with Vendor supported versions of Edge, Chrome, Safari, and Firefox browsers. Silverlight, QuickTime, PHP, Adobe ColdFusion, and Adobe Flash will not be used in the system, site, or application. Adobe Animate CC is allowed if files that require third-party plugins are not required.

Section XXIII. Security Acknowledgment Form

The Vendor will be required to sign the Security Acknowledgement Form which is attached to this Agreement as Exhibit ______. The signed Security Acknowledgement Form must be submitted to the State and approved by the South Dakota Bureau of Information and Telecommunications and communicated to the Vendor by the State contact before work on the contract may begin. This Security Acknowledgment Form constitutes the agreement of the Vendor to be responsible and liable for ensuring that the Vendor, the Vendor's employee(s), and subcontractor's, agents, assigns and affiliated entities and all of their employee(s), participating in the work will abide by the terms of the Information Technology Security Policy (ITSP). Failure to abide by the requirements of the ITSP or the Security Acknowledgement Form can be considered a breach of this Agreement at the discretion of the State. It is also a breach of this Agreement, at the discretion of the State, if the Vendor does not sign another Security Acknowledgement Form covering any employee(s) and any subcontractor's, agent's, assign's, or affiliated entities' employee(s), any of whom are participating in the work covered by this Agreement, and who begin working under this Agreement after the project has begun. Any disciplining of the Vendor's, Vendor's employee(s), or subcontractor's, agent's, assign's, or affiliated entities' employee(s) due to a failure to abide by the terms of the Security Acknowledgement Form will be done at the discretion of the Vendor or subcontractors, agents, assigns, or affiliated entities and in accordance with the Vendor's or subcontractor's, agent's, assign's, and affiliated entities' personnel policies. Regardless of the actions taken by the Vendor and subcontractors, agents, assigns, and affiliated entities, the State will retain the right to require at the State's discretion the removal of the employee(s) from the project covered by this Agreement.

Section XXIV. Information Technology Standards

Any service, software, or hardware provided under this Agreement will comply with State standards which can be found at https://bit.sd.gov/bit?id=bit_standards_overview.

Section XXV. Product Usage

The State cannot be held liable for any additional costs or fines for mutually understood product usage over and above what has been agreed to in this Agreement unless there has been an audit conducted on the product usage. This audit must be conducted using a methodology agreed to by the State. The results of the audit must also be agreed to by the State before the State can be held to the results. Under no circumstances will the State be required to pay for the costs of said audit.

Section XXVI. Security

The Vendor must take all actions necessary to protect State information from exploits, inappropriate alterations, access or release, and malicious attacks.

By signing this Agreement, the Vendor warrants that:

A. All Critical, High, Medium, and Low security issues are resolved. Critical, High, Medium, and Low can be described as follows:

1. **Critical** - Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices.
2. **High** - The vulnerability is difficult to exploit; however, it is possible for an expert in Information Technology. Exploitation could result in elevated privileges.
3. **Medium** - Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. Denial of service vulnerabilities that are difficult to set up.
4. **Low** - Vulnerabilities identified by the State as needing to be resolved that are not Critical, High, or Medium issues.

B. Assistance will be provided to the State by the Vendor in performing an investigation to determine the nature of any security issues that are discovered or are reasonably suspected after acceptance. The Vendor will fix or mitigate the risk based on the following schedule: Critical and high risk, within 7 days, medium risk within 14 days, low risk, within 30 days.

Section XXVII. Security Scanning

The State routinely applies security patches and security updates as needed to maintain compliance with industry best practices as well as state and federal audit requirements. Vendors who do business with the State must also subscribe to industry security practices and requirements. Vendor s must include costs and time needs in their proposals and project plans to assure they can maintain currency with all security needs throughout the lifecycle of a project. The State will collaborate in good faith with the Vendor to help them understand and support State security requirements during all phases of a project's lifecycle but will not assume the costs to mitigate applications or processes that fail to meet then-current security requirements.

At the State's discretion, security scanning will be performed and security settings will be put in place or altered during the software development phase and during pre-production review for new or updated code. These scans and tests, initially applied to development and test environments, can be time consuming and should be accounted for in project planning documents and schedules. Products not meeting the State's security and performance requirements will not be allowed into production and will be barred from User Acceptance Testing (UAT) until all issues are addressed to the State's satisfaction. The discovery of security issues during UAT are automatically sufficient grounds for non-acceptance of a product even though a product may satisfy all other acceptance criteria. Any security issues discovered during UAT that require product changes will not be considered a project change chargeable to the State. The State urges the use of industry scanning/testing tools and recommends secure development methods are employed to avoid unexpected costs and project delays. Costs to produce and deliver secure and reliable applications are the responsibility of the Vendor 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.

Section XXVIII. Malicious Code

A. The Vendor warrants that the Agreement deliverables contain no code that does not support an application requirement.
B. The Vendor warrants that the Agreement deliverables contains no malicious code.
C. The Vendor warrants that the Vendor will not insert into the Agreement deliverables or any media on which the Agreement deliverables is delivered any malicious or intentionally destructive code.
D. In the event any malicious code is discovered in the Agreement deliverables, the Vendor must provide the State at no charge with a copy of or access to the applicable Agreement deliverables that contains no malicious code or otherwise correct the affected portion of the services provided to the State. The remedies in this Section are in addition to other additional remedies available to the State.

Section XXIX. Denial of Access or Removal of Application or Hardware from Production

During the life of this Agreement the application and hardware can be denied access to or removed from production at the State's discretion. The reasons for the denial of access or removal of the application or hardware from the production system may include but not be limited to security, functionality, unsupported third-party technologies, or excessive resource consumption. Denial of access or removal of an application or hardware also may be done if scanning shows that any updating or patching of the software and or hardware produces what the State determines are unacceptable results.

The Vendor will be liable for additional work required to rectify issues concerning security, functionality, unsupported third-party technologies, and excessive consumption of resources if it is for reasons of correcting security deficiencies or meeting the functional requirements originally agreed to for the application or hardware. At the discretion of the State, contractual payments may be suspended while the application or hardware is denied access to or removed from production. The reasons can be because of the Vendor's actions or inactions. Access to the production system to perform any remedying of the reasons for denial of access or removal of the software and hardware, and its updating and or patching will be made only with the State's prior approval.

It is expected that the Vendor will provide the State with proof of the safety and effectiveness of the remedy, update, or patch proposed before the State provides access to the production system. The State will sign a non-disclosure agreement with the Vendor if revealing the update or patch will put the Vendor's intellectual property at risk. If the remedy, update, or patch the Vendor proposes is unable to present software or hardware that meets the State's requirements, as defined by the State, which may include but is not limited to security, functionality, or unsupported third party technologies, to the State's satisfaction within 30 days of the denial of access to or removal from the production system and the Vendor does not employ the change management process to alter the project schedule or deliverables within the same 30 days then at the State's discretion the Agreement may be terminated.

Section XXX. Movement of Product

The State operates a virtualized computing environment and retains the right to use industry standard hypervisor high availability, fail-over, and disaster recovery systems to move instances of the product(s) between the install sites defined with the Vendor within the provisions of resource and usage restrictions outlined elsewhere in the Agreement. As part of normal operations, the State may also install the product on different computers or servers if the product is also removed from the previous computer or server within the provisions of resource and usage restrictions outlined elsewhere in the Agreement. All such movement of product can be done by the State without any additional fees or charges by the Vendor.

Section XXXI. Use of Product on Virtualized Infrastructure and Changes to that Infrastructure

The State operates a virtualized computing environment and uses software-based management and resource capping. The State retains the right to use and upgrade as deemed appropriate its hypervisor and operating system technology and related hardware without additional license fees or other charges provided the State assures the guest operating system(s) running within that hypervisor environment continue to present computing resources to the licensed product in a consistent manner. The computing resource allocations within the State's hypervisor software-based management controls for the guest operating system(s) executing the product will be the only consideration in licensing compliance related to computing resource capacity.

Section XXXII. Load Balancing

The State routinely load balances across multiple servers, applications that run on the State's computing environment. The Vendor's product must be able to be load balanced across multiple servers. Any changes or modifications required to allow the Vendor's product to be load balanced so that it can operate on the State's computing environment will be at the Vendor's expense.

Section XXXIII. Backup Copies

The State may make and keep backup copies of the licensed product without additional cost or obligation on the condition that:

A. The State maintains possession of the backup copies.

B. The backup copies are used only as bona fide backups.

Section XXXIV. Use of Abstraction Technologies

The Vendor's application must use abstraction technologies in all applications, that is the removal of the network control and forwarding functions that allows the network control to become directly programmable and the underlying infrastructure to be separated for applications and network services.

The Vendor warrants that hard-coded references will not be used in the application. Use of hard-coded references will result in a failure to pass pre-production testing or may cause the application to fail or be shut down at any time without warning and or be removed from production. Correcting the hardcoded references is the responsibility of the Vendor and will not be a project change chargeable to the State. If the use of hard-coded references is discovered after User Acceptance Testing the Vendor will correct the problem at no additional cost.

Section XXXV. Scope of Use

A. There will be no limit on the number of locations, or size of processors on which the State can operate the software.
B. There will be no limit on the type or version of operating systems upon which the software may be used.

Section XXXVI. Web and Mobile Applications

A. The Vendor's application is required to:

1. have no code or services including web services included in or called by the application unless they provide direct, functional requirements that support the State's business goals for the application,
2. encrypt data in transport and at rest using a mutually agreed upon encryption format,
3. close all connections and close the application at the end of processing,
4. have documentation that is in grammatically complete text for each call and defined variables (i.e., using no abbreviations and using complete sentences) sufficient for a native speaker of English with average programming skills to determine the meaning or intent of what is written without prior knowledge of the application,
5. have no code not required for the functioning of application,
6. have no "back doors", a back door being a means of accessing a computer program that bypasses security mechanisms, or other entries into the application other than those approved by the State,
7. permit no tracking of device user's activities without providing a clear notice to the device user and requiring the device user's active approval before the application captures tracking data,
8. have no connections to any service not required by the functional requirements of the application or defined in the project requirements documentation,
9. fully disclose in the "About" information that is the listing of version information and legal notices, of the connections made, permission(s) required, and the purpose of those connections and permission(s),
10. ask only for those permissions and access rights on the user's device that are required for the defined requirements of the Vendor's application,

11. access no data outside what is defined in the “About” information for the Vendor’s application,
12. conform to Web Content Accessibility Guidelines 2.0,
13. have Single Sign On capabilities with the State’s identity provider,

If the application does not adhere to the requirements given above or the Vendor has unacceptable disclosures, at the State’s discretion, the Vendor will rectify the issues at no cost to the State.

Section XXXVII. Intended Data Access Methods

The Vendor’s application will not allow a user, external to the State’s domain, to bypass logical access controls required to meet the application’s functional requirements. All database queries using the Vendor’s application can only access data by methods consistent with the intended business functions.

If the State can demonstrate the application flaw, to the State’s satisfaction, then the Vendor will rectify the issue, to the State’s satisfaction, at no cost to the State.

Section XXXVIII. Application Programming Interface

Vendor documentation on application programming interface must include a listing of all data types, functional specifications, a detailed explanation on how to use the Vendor’s application programming interface and tutorials. The tutorials must include working sample code.

Section XXXIX. Access to Source and Object Code

The Vendor will provide access to source and object code for all outward facing areas of the system where information is presented, shared, or received whether via browser-based access and programmatic-based access including but not limited to application program interfaces (APIs) or any other access or entry point accessible via the world wide web, modem, or other digital process that is connected to a digital network, radio-based or phone system.

Section XL. Data Location and Offshore Services

The Vendor must provide its services to the State as well as storage of State Data solely from data centers located in the continental United States. The Vendor will not provide access to State Data to any entity or person(s) located outside the continental United States that are not named in this Agreement without prior written permission from the State. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States.

Section XLI. Vendor Training Requirements

The Vendor, Vendor’s employee(s), and Vendor’s subcontractors, agents, assigns, affiliated entities and their employee(s), must successfully complete, at the time of hire a cyber-security training program. The training must include but is not limited to:

A. legal requirements for handling data,
B. media sanitation,
C. strong password protection,

D. social engineering, or the psychological manipulation of persons into performing actions that are inconsistent with security practices or that cause the divulging of confidential information, and

E. security incident response.

Section XLII. Data Sanitization

At the end of the project covered by this Agreement the Vendor, and Vendor's subcontractors, agents, assigns, and affiliated entities will return the State Data or securely dispose of all State Data in all forms, this can include State Data on media such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs. This State Data must be permanently deleted by either purging the data or destroying the medium on which the State Data is found according to the methods given in the most current version of NIST 800-88. Certificates of Sanitization for Offsite Data (See bit.sd.gov/vendor/default.aspx for copy of certificate) must be completed by the Vendor and given to the State contact. The State will review the completed Certificates of Sanitization for Offsite Data. If the State is not satisfied by the data sanitization then the Vendor will use a process and procedure that does satisfy the State.

This contract clause remains in effect for as long as the Vendor, and Vendor's subcontractors, agents, assigns, and affiliated entities have the State data, even after the Agreement is terminated or the project is completed.

Section XLIII. Banned Hardware and Software

The Vendor will not provide to the State any computer hardware or video surveillance hardware, or any components thereof, or any software that was manufactured, provided, or developed by a covered entity. As used in this paragraph, "covered entity" means the following entities and any subsidiary, affiliate, or successor entity and any entity that controls, is controlled by, or is under common control with such entity: Kaspersky Lab, Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, or any entity that has been identified as owned or controlled by, or otherwise connected to, People's Republic of China. The Vendor will immediately notify the State if the Vendor becomes aware of credible information that any hardware, component, or software was manufactured, provided, or developed by a covered entity.

Section XLIV. Use of Portable Devices

The Vendor must prohibit its employees, agents, affiliates, and subcontractors from storing State Data on portable devices, including personal computers, except for devices that are used and kept only at the Vendor's data center(s). All portable devices used for storing State Data must be password protected and encrypted.

Section XLV. Remote Access

The Vendor will prohibit its employees, agents, affiliates, and subcontractors from accessing State Data remotely except as necessary to provide the services under this Agreement and consistent with all contractual and legal requirements. The accounts used for remote access cannot be shared accounts and must include multifactor authentication. If the State Data that is being remotely accessed is legally protected data or considered sensitive by the State, then:

A. The device used must be password protected,

B. The data is not put onto mobile media (such as flash drives),
C. No non-electronic copies are made of the data, and
D. A log must be maintained by the Vendor detailing the data which was accessed, when it was accessed, and by whom it was accessed.

The Vendor must follow the State's data sanitization standards, as outlined in this Agreement's Data Sanitization clause, when the remotely accessed data is no longer needed on the device used to access the data.

Section XLVI. Data Encryption

If State Data will be remotely accessed or stored outside the State's IT infrastructure, the Vendor warrants that the data will be encrypted in transit (including via any web interface) and at rest at no less than AES256 level of encryption with at least SHA256 hashing.

Section XLVII. Rights, Use, and License of and to State Data

The parties agree that all rights, including all intellectual property rights, in and to State Data will remain the exclusive property of the State. The State grants the Vendor a limited, nonexclusive license to use the State Data solely for the purpose of performing its obligations under this Agreement. This Agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the Agreement.

Protection of personal privacy and State Data must be an integral part of the business activities of the Vendor to ensure there is no inappropriate or unauthorized use of State Data at any time. To this end, the Vendor must safeguard the confidentiality, integrity, and availability of State Data and comply with the following conditions:

A. The Vendor will implement and maintain appropriate administrative, technical, and organizational security measures to safeguard against unauthorized access, disclosure, use, or theft of Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI), or any information that is confidential under applicable federal, state, or international law, rule, regulation, or ordinance. Such security measures will be in accordance with recognized industry practice and not less protective than the measures the Vendor applies to its own non-public data.
B. The Vendor will not copy, disclose, retain, or use State Data for any purpose other than to fulfill its obligations under this Agreement.
C. The Vendor will not use State Data for the Vendor's own benefit and will not engage in data mining of State Data or communications, whether through automated or manual means, except as specifically and expressly required by law or authorized in writing by the State through a State employee or officer specifically authorized to grant such use of State Data.

Section XLVIII. Software License

The State grants the Vendor a nonexclusive, worldwide, revocable, fully paid, nontransferable license to all code provided to the Vendor and all modifications to the licensed code, which becomes property of the State, pursuant to this Agreement. The license rights granted in this Agreement will continue so long as the Parties are under a contract regarding the licensed code.

A. The State grants the Vendor the right to:

1. use the licensed code for only the State's benefit pursuant to this Agreement,
2. make as many copies of the licensed code as necessary to fulfill its obligations under this Agreement,
3. modify the licensed code pursuant to the terms of this Agreement,
4. publicly perform the licensed code, if applicable; and
5. publicly display the licensed code, if applicable.

B. The Vendor is not granted the following rights and is prohibited from doing the following:

1. creating derivative works from the licensed code,
2. distributing the licensed code, and
3. sublicensing the licensed code.

Copies of the licensed code created or transferred pursuant to this Agreement are licensed to the Vendor, not sold. The Vendor receives no title to or ownership of any copy or of the licensed code itself. Furthermore, the Vendor receives no rights to the licensed code other than those specifically granted in this Agreement.

Section XLIX. Transfer of Ownership of Work Product

Upon the effective date of this Agreement, the Vendor hereby assigns to the State all of the Vendor's ownership, right, title, and interest in and to any copyrights in any code and other assets created pursuant this Agreement ("Work Product"), including all modifications to the licensed code provided to the Vendor by the State. All modifications to the licensed code become part of the licensed code once accepted by the State and is subject to all the aspects of this Agreement regarding "licensed code."

A. **License.** To the extent that this Section does not provide the State with full ownership, right, title, and interest in and to the Work Product, the Vendor hereby grants the State a perpetual, irrevocable, fully paid, royalty-free, worldwide license to reproduce, create derivative works from, distribute, publicly display, publicly perform, and use the Work Product, with the right to sublicense each such right.

B. **Further Assistance and Survival.** The Vendor will reasonably assist the State in obtaining and enforcing copyrights in the Work Product, at the State's expense. The rights granted in this Section will survive any termination or expiration of this Agreement.

C. **Transfer of Employee Rights.** Prior to the effective date of this Agreement, the Vendor will ensure that all its employees and contractors who may in any way be involved in creating the Work Product are subject to written agreements with the Vendor that grants the Vendor all such employees' or contractors' present and future ownership and other rights in and to the Work Product.

Section L. Third Party Hosting

If the Vendor has the State's data hosted by another party, the Vendor must provide the State the name of this party. The Vendor must provide the State with contact information for this third party and the location of their data center(s). The Vendor must receive from the third party written assurances that the State's data will always reside in the continental United States and provide these written assurances to the State. This restriction includes the data being viewed or accessed by the third-party's employees or contractors. If during the term of this Agreement the Vendor changes from the Vendor hosting the data to a third-party hosting the data or changes third-party hosting provider, the Vendor will provide the State with 180 days' advance notice of this change and at that time provide the State with the information required above.

Section LI. Securing of Data

All facilities used to store and process State Data will employ industry best practices, including appropriate administrative, physical, and technical safeguards to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the Vendor's own data of a similar type, and in no event less than commercially reasonable in view of the type and nature of the data involved.

Section LII. Security Processes

The Vendor will disclose its non-proprietary security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the Vendor. For example: virus checking and port sniffing.

Section LIII. Import and Export of Data

The State will have the ability to import or export data piecemeal or in entirety at its discretion without interference from the Vendor. This includes the ability for the State to import or export data to/from other vendors.

Section LIV. System Upgrades

The Vendor must provide advance notice of 30 days to the State of any major upgrades or system changes the Vendor will be implementing unless the changes are for reasons of security. A major upgrade is a replacement of hardware, software, or firmware with a newer or improved version, in order to bring the system up to date or to improve its characteristics. The State reserves the right to postpone these changes unless the upgrades are for security reasons. The State reserves the right to scan the Vendor's systems for vulnerabilities after a system upgrade. These vulnerability scans can include penetration testing of a test system at the State's discretion.

Section LV. Use of Production Data in a Non-Production Environment

The Vendor cannot use protected State Data, whether legally protected or protected by industry standards, in a non-production environment. Any non-production environment that is found to have legally protected production data, must be purged immediately and the State contact notified. The State will decide if this event is to be considered a security incident. "Legally protected production data" is any data protected under federal or state statute or regulation. "Industry standards" are data handling requirements specific to an industry. An example of data protected by industry standards is payment card industry information (PCI). Protected data that is de-identified, aggregated, or hashed is no longer considered to be legally protected.

Section LVI. Banned Services

The Vendor warrants that any hardware or hardware components used to provide the services covered by this Agreement were not manufactured by Huawei Technologies Company or ZTE

Corporation, or any subsidiary or affiliate of such entities. Any company considered to be a security risk by the government of the United States under the International Emergency Economic Powers Act or in a United States appropriation bill will be included in this ban.

Section LVII. Multifactor Authentication for Hosted Systems

If the Vendor is hosting on their system or performing Software as a Service where there is the potential for the Vendor or the Vendor's subcontractor to see protected State Data, then Multifactor Authentication (MFA) must be used to before this data can be accessed. The Vendor's MFA, at a minimum must adhere to the requirements of *Level 3 Authentication Assurance for MFA* as defined in NIST 800-63.

Attachment B
Security and Vendor Questions

Agencies: The following questions facilitate agencies acquiring technology that meets state security standards. These questions will assist in improving the quality and the timeliness of the procurement. The Bureau of Information and Telecommunications (BIT) recommends that you utilize your BIT Point of Contact (POC) to set up a planning meeting to review the project and these questions. Understanding the background and context of the questions greatly improves realizing the purpose of the questions. Again, the purpose of the questions is to ensure the product/service being procured will meet the technology and security standards of the state.

If you do not know the details of the technologies the vendor will propose, it is best to keep the question set as broad as possible. If there is a detailed knowledge of what will be proposed, a narrowed set of questions may be possible. Vendors are invited to mark any question that does not apply to their technology as NA (Not Applicable).

Vendors: The following questions help the state determine the best way to assess and integrate your product or service technology with the state's technology infrastructure. Some questions may not apply to the technology you use. In such cases, simply mark the question as NA (Not Applicable). The questions are divided into sections to help identify the point of the questions.

Use the last column as needed to explain your response. Also note, many questions require you to explain your response. The more detailed the response, the better we can understand your product or service.

Where we feel that a Yes/No/NA response is not appropriate, the cell has been grayed out. **If the vendor answers a question by referencing another document or another part of the RFP response, the vendor must provide the page number and paragraph where the information can be found.**

The "BIT" column corresponds to the division within BIT that will be the primary reviewers. If you have questions about the meaning or intent of a question, we can contact the BIT division on your behalf. DC = Data Center; DEV = Development; TEL = Telecommunications; POC = Point of Contract.

System/Product:
The following questions are relevant for all vendors or third parties engaged in this hardware, software, application, or service.

			Response
#	**BIT**	**Question**	**Select all that apply**
1	DC DEV	Is your proposed solution a cloud-based solution or an on-prem solution?	☐ State Hosted On-prem (dedicated VM/infrastructure) ☐ State Cloud Provider (PaaS Solution) ☐ Vendor Hosted
2	DC DEV TEL	What type of access is required by vendor or proposed solution to state hosted or external resources?	☐ Not Required ☐ VPN ☐ API ☐ SFTP ☐ Other: (Please state)
3	DC	What type of access is required by vendor to maintain and support the solution?	☐ Not Required ☐ Citrix (For On-prem) ☐ State Cloud Access ☐ Other: (Please state)
4	TEL	If an on-prem solution, which of the following will apply?	☐ IoT Hardware ☐ Non-Windows or non-domain joined solution ☐ Windows-based domain joined hardware ☐ Other: (Please state)
5	DC TEL	Does your proposed solution include/require additional devices connected to the application for activities such as scanning or printing?	☐ Yes ☐ No

6	DC	Does the proposed solution include the use of email?	☐ Yes ☐ No
7	POC TEL	Will there be any desktop software installs, policies, or software required on state managed computers as part of this product?	☐ Yes ☐ No If "Yes", please define:
8	POC	If there are desktop software installs, please provide a link to the licensing requirements or a copy of the licensing requirements.	Please provide link below, if applicable:
9	POC	Will any hardware or peripherals need to be attached to or added to state managed computers?	☐ Yes ☐ No If "Yes", please define:
10	POC	Will any browser plugins be required to install, access, or use this product?	☐ Yes ☐ No If "Yes", please define:
11	POC	Will any products that connect or interact with a state managed computer or network be required as part of this product or project?	☐ Yes ☐ No If "Yes", please define:
12	POC	Will any Bluetooth or RF frequency devices be required as part of this product or project?	☐ Yes ☐ No If "Yes", please define:
13	POC	What operating system is the software/hardware compatible with?	☐ Microsoft Windows 10 ☐ Microsoft Windows 11 ☐ Other (please specify): ☐ N/A

Section A. System Security **The following questions are relevant for all vendors or third parties engaged in this hardware, application, or service and pertain to relevant security practices and procedures.**						
			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
A1	DC	Does the solution require user authentication, and does that authentication solution support OpenID Connect or OAUTH2 to provide single sign-on?				
A2	DC TEL x	Will the system provide internet security functionality on public portals using encrypted network/secure socket layer connections in line with current recommendations of the Open Web Application Security Project (OWASP)?				
A3	POC	Will the system have role-based access?				
A4	DC TEL	Does the application contain mitigations for risks associated to uncontrolled login attempts (response latency, re-Captcha, lockout, IP filtering, multi-factor authentication)? Which mitigations are in place? What are the optional mitigations?				

A5	DC TEL	Are account credentials hashed and encrypted when stored?				
A6	DC TEL x	The protection of the State's system and data is of upmost importance. Security 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 State would want to scan a test system; not a production system and will not do penetration testing.** The scanning will be done with industry standard tools. Scanning would also take place annually as well as when there are code changes. Are either of these an issue? If so, please explain.				
A7	DC	Will SSL traffic be decrypted and inspected before it is allowed into your system?				
A8	POC x	Will organizations other than the State of South Dakota have access to our data?				
A9	DEV TEL	Do you have developers that possess software security related certifications (e.g., the SANS secure coding certifications)?				
A10	DEV	Are there some requirements for security that are "structured" as part of general release readiness of a product, and others that are "as needed" or "custom" for a particular release?				
A11	TEL	What threat assumptions were made, if any, when designing protections for the software and information assets processed?	▨	▨		
A12	TEL	How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used?	▨	▨		
A13	TEL	What security criteria, if any, are considered when selecting third party suppliers?	▨	▨		
A14	TEL	How has the software been measured/assessed for its resistance to publicly known vulnerabilities and/or attack patterns identified in the Common Vulnerabilities & Exposures (CVE®) or Common Weakness Enumerations (CWEs)? How have the findings been mitigated?	▨	▨		

A15	TEL	Has the software been evaluated against the Common Criteria, FIPS 140-2, or other formal evaluation process? If so, please describe what evaluation assurance level (EAL) was achieved, what protection profile the product claims conformance to, and indicate if the security target and evaluation report are available.				
A16	DC TEL	Are static or dynamic software security analysis tools used to identify weaknesses in the software that can lead to exploitable vulnerabilities? If yes, which tools are used? What classes of weaknesses are covered? When in the SDLC are these scans performed? Are SwA experts involved in the analysis of the scan results?				
A17	DC TEL x	Has the product undergone any vulnerability and/or penetration testing? If yes, how frequently, by whom, and are the test reports available under a nondisclosure agreement? How have the findings been mitigated?				
A18	DC	Does your company have an executive-level officer responsible for the security of your company's software products and/or processes?				
A19	DC	How are software security requirements developed?	▨	▨		
A20	DC	What risk management measures are used during the software's design to mitigate risks posed by use of third-party components?	▨	▨		
A21	DC	What is your background check policy and procedure? Are your background checks fingerprint based?				
A22	DEV	Does your company have formally defined security policies associated with clearly defined roles and responsibilities for personnel working within the software development life cycle? Explain.				
A23	TEL	What are the policies and procedures used to protect sensitive information from unauthorized access? How are the policies enforced?	▨	▨		
A24	DC TEL	Do you have an automated Security Information and Event Management system?				
A25	DC TEL	What types of event logs do you keep and how long do you keep them?				
		a. System events	▨	▨		
		b. Application events	▨	▨		
		c. Authentication events	▨	▨		
		d. Physical access to your data center(s)	▨	▨		
		e. Code changes	▨	▨		

		f. Other:	▨	▨		
A26	DC	How are security logs and audit trails protected from tampering or modification? Are log files consolidated to single servers?				
A27	DEV	a. Are security specific regression tests performed during the development process?				
		b. If yes, how frequently are the tests performed?	▨	▨		
A28	TEL	What type of firewalls (or application gateways) do you use? How are they monitored/managed?	▨	▨		
A29	TEL	What type of Intrusion Detection System/Intrusion Protection Systems (IDS/IPS) do you use? How are they monitored/managed?	▨	▨		
A30	DC TEL	What are your procedures for intrusion detection, incident response, and incident investigation and escalation?	▨	▨		
A31	DC TEL	Do you have a BYOD policy that allows your staff to put any sort of sensitive or legally protected State data on their device personal device(s) or other non-company owned system(s)?				
A32	DC TEL	Do you require multifactor authentication be used by employees and subcontractors who have potential access to legally protected State data or administrative control? If yes, please explain your practices on multifactor authentication including the authentication level used as defined in NIST 800-63 in your explanation. If no, do you plan on implementing multifactor authentication? If so, when?	▨	▨		
A33	POC	Will this system provide the capability to track data entry/access by the person, date, and time?				
A34	DC DEV POC TEL	Will the system provide data encryption for sensitive or legally protected information both at rest and transmission? If yes, please provide details.				
A35	DC	a. Do you have a SOC 2 or ISO 27001 audit report?				
		b. Is the audit performed annually?				
		c. If it is SOC 2 audit report, does it cover all 5 of the trust principles?				
		d. If it is a SOC 2 audit report, what level is it?				
		e. Does the audit include cloud service providers?				
		f. Has the auditor always been able to attest to an acceptable audit result?				

		g. Will you provide a copy of your latest SOC 2 or ISO 27001 audit report upon request? A redacted version is acceptable.				
A36	DC	Do you or your cloud service provider have any other security certification beside SOC 2 or ISO 27001, for example, FedRAMP or ITTRUST?				
A37	DC TEL	Are you providing a device or software that can be defined as being Internet of Thing (IoT)? Examples include IP camera, network printer, or connected medical device. If yes, what is your process for ensuring the software on your IoT devices that are connected to the state's system, either permanently or intermittently, are maintained and/or updated?				
A38	DC	Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all registry settings?				
A39	DC	What are your policies and procedures for hardening servers?				
A40	DC TEL	**(Only to be used when medical devices are being acquired.)** Please give the history of cybersecurity advisories issued by you for your medical devices. Include the device, date, and the nature of the cybersecurity advisory.				
A41	DC POC	Does any product you propose to use or provide the State include software, hardware, or hardware components manufactured by any company on the US Commerce Department's Entity List?				
A42	DC	Describe your process for monitoring the security of your suppliers.				

Section B. Hosting

The following questions are relevant to any hosted applications, systems, databases, services, and any other technology. The responses should not assume a specific hosting platform, technology, or service but instead the response should address any hosting options available for the proposed solution.

For state-hosted systems that reside in a state-managed cloud:

To minimize impacts to project schedules, vendors are required to provide architectural plans, resource needs, permission plans, and all interfaces – both internal to the state and internet facing for cloud hosted systems. The documentation provided will be reviewed as part of the initial assessment process. If selected for award of a contract, and once the state has approved the submitted materials, a test environment will be provided after contract signature. Systems will be reviewed again before being moved to a production environment. Any usage or processes that are deemed out of compliance with what was approved or represent excessive consumption or risk will require remediation before being moved to production.

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
B1	POC	Are there expected periods of time where the application will be unavailable for use?				
B2	DC	If you have agents or scripts executing on servers of hosted applications what are the procedures for reviewing the security of these scripts or agents?				

B3	DC	What are the procedures and policies used to control access to your servers? How are audit logs maintained?	▨	▨		
B4	DC DEV POC TEL	Do you have a formal disaster recovery plan? Please explain what actions will be taken to recover from a disaster. Are warm or hot backups available? What are the Recovery Time Objectives and Recovery Point Objectives?				
B5	DC	Explain your tenant architecture and how tenant data is kept separately?	▨	▨		
B6	DC	What are your data backup policies and procedures? How frequently are your backup procedures verified?	▨	▨		
B7	DC DEV TEL	If any cloud services are provided by a third-party, do you have contractual requirements with them dealing with: • Security for their I/T systems; • Staff vetting; • Staff security training?				
		a. If yes, summarize the contractual requirements.	▨	▨		
		b. If yes, how do you evaluate the third-party's adherence to the contractual requirements?	▨	▨		
B8	DC	If your application is hosted by you or a third party, are all costs for your software licenses in addition to third-party software (i.e. MS-SQL, MS Office, and Oracle) included in your cost proposal? If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized?				
B9	DC	a. Do you use a security checklist when standing up any outward facing system?				
		b. Do you test after the system was stood up to make sure everything in the checklist was correctly set?				
B10	DC	How do you secure Internet of Things (IoT) devices on your network?	▨	▨		
B11	DC TEL	Do you use Content Threat Removal to extract and transform data?				
B12	DC TEL	Does your company have an endpoint detection and response policy?				
B13	DC TEL	Does your company have any real-time security auditing processes?				
B14	TEL	How do you perform analysis against the network traffic being transmitted or received by your application, systems, or data center? What benchmarks do you maintain and monitor your systems against for network usage and performance? What process(es) or product(s) do you use to complete this analysis, and what results or process(es) can you share?	▨	▨		
B15	TEL	How do you monitor your application, systems, and data center for security events, incidents, or information? What process(es) and/or product(s) do you use to complete this analysis, and what results or process(es) can you share?				
B16	DC	What anti-malware product(s) do you use?	▨	▨		

	TEL					
B17	DC TEL	What is your process to implement new vendor patches as they are released and what is the average time it takes to deploy a patch?				
B18	DC TEL	Have you ever had a data breach? If so, provide information on the breach.				
B19	POC	Is there a strategy for mitigating unplanned disruptions and what is it?				
B20	DC TEL	What is your process for ensuring the software on your IoT devices that are connected to your system, either permanently or intermittently, is maintained and updated?				
B21	POC	Will the State of South Dakota own the data created in your hosting environment?				
B22	DEV	What are your record destruction scheduling capabilities?				

Section C: Database
The following questions are relevant to any application or service that stores data, irrespective of the application being hosted by the state or the vendor.

						Response
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
C1	DC	Will the system require a database?				
C2	DC	If a Database is required, what technology will be used (i.e. Microsoft SQL Server, Oracle, MySQL)?				
C3	DC	If a SQL Database is required does the cost of the software include the cost of licensing the SQL Server?				
C4	POC	Will the system data be exportable by the user to tools like Excel or Access at all points during the workflow?				
C5	DC DEV	Will the system infrastructure include a separate OLTP or Data Warehouse Implementation?				
C6	DC DEV	Will the system infrastructure require a Business Intelligence solution?				

Section D: Contractor Process
The following questions are relevant for all vendors or third parties engaged in providing this hardware, application, or service and pertain to business practices. If the application is hosted by the vendor or the vendor supplies cloud services those questions dealing with installation or support of applications on the State's system can be marked "NA".

						Response
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
D1	DC POC	Will the vendor provide assistance with installation?				
D2	DC DEV POC TEL	Does your company have a policy and process for supporting/requiring professional certifications? If so, how do you ensure certifications are valid and up-to date?				
D3	DEV	What types of functional tests are/were performed on the software during its development (e.g., spot checking, component-level testing, and integrated testing)?				
D4	DEV	Are misuse test cases included to exercise potential abuse scenarios of the software?				

D5	TEL	What release criteria does your company have for its products regarding security?				
D6	DEV	What controls are in place to ensure that only the accepted/released software is placed on media for distribution?				
D7	DC DEV	a. Is there a Support Lifecycle Policy within the organization for the software				
		b. Does it outline and establish a consistent and predictable support timeline?				
D8	DC	How are patches, updates, and service packs communicated and distributed to the State?				
D9	DEV	What services does the help desk, support center, or (if applicable) online support system offer when are these services available, and are there any additional costs associated with the options?				
D10	DC	a. Can patches and service packs be uninstalled?				
		b. Are the procedures for uninstalling a patch or service pack automated or manual?				
D11	DC DEV	How are enhancement requests and reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, prioritized, and reported? Is the management and reporting policy available for review?				
D12	DC	What are your policies and practices for reviewing design and architecture security impacts in relation to deploying patches, updates, and service packs?				
D13	DC	Are third-party developers contractually required to follow your configuration management and security policies and how do you assess their compliance?				
D14	DEV	What policies and processes does your company use to verify that your product has its comments sanitized and does not contain undocumented functions, test/debug code, or unintended, “dead,” or malicious code? What tools are used?				
D15	DEV	How is the software provenance verified (e.g., any checksums or signatures)?				
D16	DEV	a. Does the documentation explain how to install, configure, and/or use the software securely?				
		b. Does it identify options that should not normally be used because they create security weaknesses?				
D17	DEV	a. Does your company develop security measurement objectives for all phases of the SDLC?				
		b. Has your company identified specific statistical and/or qualitative analytical techniques for measuring attainment of security measures?				
D18	DC	a. Is testing done after changes are made to servers?				
		b. What are your rollback procedures in the event of problems resulting from installing a patch or service pack?				
D19	DC	What are your procedures and policies for handling and destroying sensitive data on electronic and printed media?				

D20	DC TEL	How is endpoint protection done? For example, is virus prevention used and how are detection, correction, and updates handled?				
D21	DC TEL	Do you perform regular reviews of system and network logs for security issues?				
D22	DC	Do you provide security performance measures to the customer at regular intervals?				
D23	DC POC	What technical, installation, and user documentation do you provide to the State? Is the documentation electronically available and can it be printed?				
D24	DC DEV POC	a. Will the implementation plan include user acceptance testing?				
		b. If yes, what were the test cases?				
		c. Do you do software assurance?				
D25	DC DEV POC TEL	Will the implementation plan include performance testing?				
D26	DEV POC	Will there be documented test cases for future releases including any customizations done for the State of South Dakota?				
D27	DEV POC	If the State of South Dakota will gain ownership of the software, does the proposal include a knowledge transfer plan?				
D28	DEV POC	Has your company ever conducted a project where your product was load tested?				
D29	DC	Please explain the pedigree of the software. Include in your answer who are the people, organization, and processes that created the software.				
D30	DC	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.				
D31	DC DEV TEL	Does your company have corporate policies and management controls in place to ensure that only corporate-approved (licensed and vetted) software components are used during the development process? **Provide a brief explanation**. Will the supplier indemnify the acquirer from these issues in the license agreement? **Provide a brief explanation.**				
D32	DEV	Summarize the processes (e.g., ISO 9000, CMMi), methods, tools (e.g., IDEs, compilers), techniques, etc. used to produce and transform the software.				
D33	DEV	a. Does the software contain third-party developed components?				
		b. If yes, are those components scanned by a static code analysis tool?				
D34	DC DEV TEL	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?				

D35	DEV	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.				
D36	DC	Does your company ever perform site inspections/policy compliance audits of its U.S. development facilities? Of its non-U.S. facilities? Of the facilities of its third-party developers? If yes, how often do these inspections/audits occur? Are they periodic or triggered by events (or both)? If triggered by events, provide examples of “trigger” events.				
D37	DC TEL	How are trouble tickets submitted? How are support issues, specifically those that are security-related escalated?				
D38	DC DEV	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. Include training specifically given to your developers on secure development.				
D39	DC TEL x	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. Would this affect the implementation of the system?				
D40	POC TEL x	Contractors are also expected to reply to follow-up questions in response to the answers they provided to the security questions. At the State’s discretion, a contractor’s answers to the follow-up questions may be required in writing and/or verbally. The answers provided may be used as part of the contractor selection criteria. Is this acceptable?				
D41	DC DEV POC TEL x	(For PHI only) a. Have you done a risk assessment? If yes, will you share it?				
		b. If you have not done a risk assessment, when are you planning on doing one?				
		c. If you have not done a risk assessment, would you be willing to do one for this project?				
D42	DEV POC	Will your website conform to the requirements of Section 508 of the Rehabilitation Act of 1973?				

Section E: Software Development

The following questions are relevant to the tools and third-party components used to develop your application, irrespective of the application being hosted by the State or the vendor.

						Response
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed.**
E1	DEV POC x	What are the development technologies used for this system? Please indicate version as appropriate.				
		ASP.Net				
		VB.Net				

		C#.Net				
		.NET Framework				
		Java/JSP				
		MS SQL				
		Other				
E2	DC TEL	Is this a browser-based user interface?				
E3	DEV POC	Will the system have any workflow requirements?				
E4	DC	Can the system be implemented via Citrix?				
E5	DC	Will the system print to a Citrix compatible networked printer?				
E6	TEL	If your application does not run under the latest Microsoft operating system, what is your process for updating the application?				
E7	DEV	Identify each of the Data, Business, and Presentation layer technologies your product would use and provide a roadmap outlining how your release or update roadmap aligns with the release or update roadmap for this technology.				
E8	TEL x	Will your system use Adobe Air, Adobe Flash, Adobe ColdFusion, Apache Flex, Microsoft Silverlight, PHP, Perl, Magento, or QuickTime? If yes, explain?				
E9	DEV	To connect to other applications or data, will the State be required to develop custom interfaces?				
E10	DEV	To fulfill the scope of work, will the State be required to develop reports or data extractions from the database? Will you provide any APIs that the State can use?				
E11	DEV POC	Has your company ever integrated this product with an enterprise service bus to exchange data between diverse computing platforms?				
E12	DC	a. If the product is hosted at the State, will there be any third-party application(s) or system(s) installed or embedded to support the product (for example, database software, run libraries)?				
		b. If yes, please list those third-party application(s) or system(s).				
E13	DEV	What coding and/or API standards are used during development of the software?				
E14	DEV	Does the software use closed-source Application Programming Interfaces (APIs) that have undocumented functions?				
E15	DEV	How does the software's exception handling mechanism prevent faults from leaving the software, its resources, and its data (in memory and on disk) in a vulnerable state?				
E16	DEV	Does the exception handling mechanism provide more than one option for responding to a fault? If so, can the exception handling options be configured by the administrator or overridden?				
E17	DEV	What percentage of code coverage does your testing provide?				
E18	DC	a. Will the system infrastructure involve the use of email?				
		b. Will the system infrastructure require an interface into the State's email infrastructure?				

		c. Will the system involve the use of bulk email distribution to State users? Client users? In what quantity will emails be sent, and how frequently?				
E19	TEL x	a. Does your application use any Oracle products?				
		b. If yes, what product(s) and version(s)?				
		c. Do you have support agreements for these products?				
E20	DC	Explain how and where the software validates (e.g., filter with whitelisting) inputs from untrusted sources before being used.				
E21	TEL	a. Has the software been designed to execute within a constrained execution environment (e.g., virtual machine, sandbox, chroot jail, single-purpose pseudo-user)?				
		b. Is it designed to isolate and minimize the extent of damage possible by a successful attack?				
E22	TEL	Does the program use run-time infrastructure defenses (such as address space randomization, stack overflow protection, preventing execution from data memory, and taint checking)?				
E23	TEL	If your application will be running on a mobile device, what is your process for making sure your application can run on the newest version of the mobile device's operating system?				
E24	DEV	Do you use open-source software or libraries? If yes, do you check for vulnerabilities in your software or library that are listed in:				
		a. Common Vulnerabilities and Exposures (CVE) database?				
		b. Open-Source Vulnerability Database (OSVDB)?				
		c. Open Web Application Security Project (OWASP) Top Ten?				

F. Infrastructure
The following questions are relevant to how your system interacts with the State's technology infrastructure. If the proposed technology does not interact with the State's system, the questions can be marked "NA".

						Response
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed.**
F1	DC	Will the system infrastructure have a special backup requirement?				
F2	DC	Will the system infrastructure have any processes that require scheduling?				
F3	DC	The State expects to be able to move your product without cost for Disaster Recovery purposes and to maintain high availability. Will this be an issue?				
F4	TEL x	Will the network communications meet Institute of Electrical and Electronics Engineers (IEEE) standard TCP/IP (IPv4, IPv6) and use either standard ports or State-defined ports as the State determines?				
F5	DC x	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?				

F6	TEL x	It is State policy that all software must be able to use either standard Internet Protocol ports or Ports as defined by the State of South Dakota BIT Network Technologies. Would this affect the implementation of the system? If yes, explain.				
F7	DC	It is State policy that all HTTP/SSL communication must be able to be run behind State of South Dakota content switches and SSL accelerators for load balancing and off-loading of SSL encryption. The State encryption is also PCI compliant. Would this affect the implementation of your system? If yes, explain.				
F8	DC x	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.				
F9	TEL x	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.				
F10	TEL	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.				
F11	TEL x	It is State policy that systems must not use dynamic Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports unless the system is a well-known one that is state firewall supported (FTP, TELNET, HTTP, SSH, etc.). Would this affect the implementation of the system? If yes, explain.				
F12	DC	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 will be offline during this scheduled maintenance time periods. Will this have a detrimental effect to the system?				
F13	POC TEL	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.				
F14	POC x	List any hardware or software you propose to use that is not State standard, the standards can be found at http://bit.sd.gov/standards/.				

F15	DC	Will your application require a dedicated environment?				
F16	DEV POC	Will the system provide an archival solution? If not, is the State expected to develop a customized archival solution?				
F17	DC TEL	Provide a system diagram to include the components of the system, description of the component, and how the components communicate with each other.				
F18	DC	Can the system be integrated with our enterprise Active Directory to ensure access is controlled?				
F19	TEL x	It is State policy that no equipment can be connected to State Network without direct approval of BIT Network Technologies. Would this affect the implementation of the system?				
F20	DC x	Will the server-based software support: a. Windows server 2016 or higher				
		b. IIS7.5 or higher				
		c. MS SQL Server 2016 standard edition or higher				
		d. Exchange 2016 or higher				
		e. Citrix XenApp 7.15 or higher				
		f. VMWare ESXi 6.5 or higher				
		g. MS Windows Updates				
		h. Carbon Black				
F21	TEL x	All network systems 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 system?				
F22	DC	All systems that require an email interface must use SMTP Authentication processes managed by BIT Datacenter. Mail Marshal is the existing product used for SMTP relay. Would this affect the implementation of the system?				
F23	DC TEL	The State implements enterprise-wide anti-virus solutions on all 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?				
F24	DC TEL	What physical access do you require to work on hardware?				
F25	DC	How many of the vendor's staff and/or subcontractors will need access to the state system, will this be remote access, and what level of access will they require?				

Section G: Business Process
The following questions pertain to how your business model interacts with the State's policies, procedures, and practices. If the vendor is hosting the application or providing cloud services, questions dealing with installation or support of applications on the State's system can be marked "NA".

						Response
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed.**
G1	DC	a. If your application is hosted on a dedicated environment within the State's infrastructure, are all costs for your software licenses in addition to third-party software (i.e. MS-SQL,				

		MS Office, and Oracle) included in your cost proposal?				
		b. If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized?				
G2	POC	Explain the software licensing model.	▨	▨		
G3	DC DEV POC	Is on-site assistance available? If so, what is the charge?				
G4	DEV POC	a. Will you provide customization of the system if required by the State of South Dakota?				
		b. If yes, are there any additional costs for the customization?				
G5	POC	Explain the basis on which pricing could change for the State based on your licensing model.	▨	▨		
G6	POC	Contractually, how many years price lock will you offer the State as part of your response? Also, as part of your response, how many additional years are you offering to limit price increases and by what percent?	▨	▨		
G7	POC	Will the State acquire the data at contract conclusion?				
G8	POC	Will the State's data be used for any other purposes other than South Dakota's usage?				
G9	DC	Has your company ever filed for Bankruptcy under U.S. Code Chapter 11? If so, please provide dates for each filing and describe the outcome.				
G10	DC	Has civil legal action ever been filed against your company for delivering or failing to correct defective software? Explain.				
G11	DC	Please summarize your company's history of ownership, acquisitions, and mergers (both those performed by your company and those to which your company was subjected).	▨	▨		
G12	DC	Will you provide on-site support 24x7 to resolve security incidents? If not, what are your responsibilities in a security incident?				
G13	DEV	What training programs, if any, are available or provided through the supplier for the software? Do you offer certification programs for software integrators? Do you offer training materials, books, computer-based training, online educational forums, or sponsor conferences related to the software?	▨	▨		
G14	DC TEL	Are help desk or support center personnel internal company resources or are these services outsourced to third parties? Where are these resources located?	▨	▨		
G15	DC	Are any of the services you plan to use located offshore (examples include data hosting, data processing, help desk, and transcription services)?				
G16	DC	Is the controlling share (51%+) of your company owned by one or more non-U.S. entities?				
G17	DC	What are your customer confidentiality policies? How are they enforced?	▨	▨		
G18	DC POC	Will this application now or possibly in the future share PHI with other entities on other networks, be				

	x	sold to another party or be accessed by anyone outside the US?				
G19	DC	If the product is hosted at the State, will there be a request to include an application to monitor license compliance?				
G20	DC POC	Is telephone assistance available for both installation and use? If yes, are there any additional charges?				
G21	DC TEL	What do you see as the most important security threats your industry faces?				