

STATE OF SOUTH DAKOTA  
**Department of Public Safety**  
118 West Capitol Avenue  
Pierre, South Dakota 57501

**South Dakota Department of Public Safety Website Redevelopment and Maintenance RFP**

**PROPOSALS ARE DUE NO LATER THAN 5PM 4/29/2024 CDT**

RFP #: 24RFP10403    BUYER: South Dakota Department of Public Safety    EMAIL: DPSinfo@state.sd.us

**READ CAREFULLY**

FIRM NAME:

AUTHORIZED SIGNATURE:

ADDRESS:

TYPE OR PRINT NAME:

CITY/STATE:

TELEPHONE NO:

ZIP (9 DIGITS):

FAX NO:

E-MAIL:

---

PRIMARY CONTACT INFORMATION

CONTACT NAME:

TELEPHONE NO:

FAX NO:

E-MAIL:

---

# 1 GENERAL INFORMATION

## 1.1 BIT STANDARD CONTRACT TERMS AND CONDITIONS

Any contract or agreement resulting from this RFP will include the State of South Dakota's (the "State") standard I/T contract terms listed in Appendix A, along with any additional contract terms as negotiated by the parties. As part of the negotiation process the contract terms listed in Appendix A may be altered or deleted. The offeror must indicate in its response any issues it has with specific contract terms. If the offeror does not indicate that there are any issues with any contract terms, then the State will assume those terms are acceptable to the offeror. There is also a list of technical questions, Security and Vendor Questions which is attached as Appendix B, the offeror must complete. These questions may be used in the proposal evaluation. It is preferred that the offeror's response to these questions is provided as a separate document from the RFP response. If the offeror 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". If the solution is not a hosted solution, the file name must be "(Your Name) Security and Vendor Questions Response". If there are multiple non-hosted solutions, please provide some designation in the file name that indicates which proposal it goes to. This document cannot be a scanned document but must be an original. If the offeror 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)

The purpose of this Request for Proposal is to solicit offerors interested in and the costs associated with building a new dynamic website, customized content management system, possible website hosting, and dedicated maintenance hours for the South Dakota Department of Public Safety, while retaining the current URL and logo. The current website is <https://dps.sd.gov/>.

## 1.3 ISSUING OFFICE AND RFP REFERENCE NUMBER

The Department of Public Safety is the issuing office for this document and all subsequent addenda relating to it, on behalf of the State of South Dakota, Department of Public Safety. The reference number for the transaction is RFP #24RFP10403. This number must be referred to on all proposals, correspondence, and documentation relating to the RFP.

## 1.4 LETTER OF INTENT

All interested offerors must submit a **Letter of Intent** to respond to this RFP.

The letter of intent must be received by the Department of Public Safety no later than 5PM CDT on April 8, 2024. If submitted by mail, the envelope should be addressed to: Attn: Dawn Hill, South Dakota Department of Public Safety, 118 West Capitol Avenue, Pierre, SD 57501.

Be sure to reference the RFP number in your letter.

The Letter of Intent may be submitted to the Department of Public Safety via email at [DPSinfo@state.sd.us](mailto:DPSinfo@state.sd.us). Please place the following in the subject line of your email: "**Letter of Intent for RFP# 24RFP10403**".

## 1.5 SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)

RFP Publication	March 28, 2024
Letter of Intent to Respond Due	April 8, 2024
Deadline for Submission of Written Inquiries	April 15, 2024
Responses to Offeror Questions	April 22, 2024
Proposal Submission	April 29, 2024
Evaluation of Proposals to Determine Short List	May 1, 2024
BIT Technical Review of Short List Submission	May 10, 2024
Demonstrations/presentations (if required)	May 21-23, 2024
Proposal Revisions (if required)	May 29, 2024
Anticipated Award Decision/Contract Negotiation	May 31, 2024
Contract Start Date	July 1, 2024
Anticipated Launch Date	No later than 3/1/2025

## 1.6 SUBMITTING YOUR PROPOSAL

All proposals must be completed and received in the Department of Public Safety's office by the date and time indicated in the Schedule of Activities.

Proposals received after the deadline will be late and ineligible for consideration.

The State will accept electronic proposals via thumb drive, which can be mailed to the Department using the specifications below.

All proposals must be signed, in ink, by an officer of the offeror, legally authorized to bind the offeror to the proposal and sealed in the form. Proposals that are not properly signed may be rejected. The sealed envelope must be marked with the appropriate RFP Number and Title. The words "Sealed Proposal Enclosed" must be prominently denoted on the outside of the shipping container.

**Proposals must be addressed and labeled as follows:**

**REQUEST FOR PROPOSAL # 24RFP10403**

**PROPOSAL TITLE South Dakota Department of Public Safety Website Redevelopment and Maintenance**

**RFP# 24RFP10403**

**PROPOSAL DUE 5PM CDT April 29, 2024**

**BUYER South Dakota Department of Public Safety**

**Attention: Dawn Hill**

**Address: 118 West Capitol Avenue, Pierre, SD 57501**

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.

## 1.7 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 offeror shall attach an explanation to its offer.

## 1.8 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.

### **1.9 RESTRICTION OF BOYCOTT OF ISRAEL**

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.

### **1.10 RESTRICTION OF PROHIBITED ENTITY**

For contractors, vendors, suppliers, or subcontractors who enter into a contract with the State of South Dakota 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, is not a prohibited 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 Codified Law § 5-18A. 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 and would be cause to suspend and debar a business under SDCL § 5-18D-12.

### **1.11 CERTIFICATION OF NO STATE LEGISLATOR INTEREST**

The bidder or offeror (i) understands neither a state legislator nor a business in which a state legislator has an ownership interest may be directly or indirectly interested in any contract with the State that was authorized by any law passed during the term for which that legislator was elected, or within one year thereafter, and (ii) has read South Dakota Constitution Article 3, Section 12 and has had the opportunity to seek independent legal advice on the applicability of that provision to any agreement entered into as a result of this RFP. By signing an agreement pursuant to this RFP, the

bidder or offeror certifies that the Agreement is not made in violation of the South Dakota Constitution Article 3, Section 12.

### **1.12 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.

### **1.13 OFFEROR INQUIRIES**

All written questions should be sent to: [DPSInfo@state.sd.us](mailto:DPSInfo@state.sd.us), only emailed questions will be accepted.

Each offeror may submit questions via email concerning this RFP to obtain clarification of requirements. No questions will be accepted after the date and time indicated in the above schedule of activities. Email questions to the email address listed above with the subject line "RFP# 24RFP10403". The questions and their answers will be sent to all offerors that submitted Letters of Intent, submitted questions, or requested the questions and answers via email before the proposal submittal date and will be sent by the date and time indicated in the above calendar of events. 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 SD RFP Project Contact. Offerors will be notified in the same manner as indicated above regarding any modifications to this RFP.

### **1.14 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. 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.

### **1.15 LENGTH OF CONTRACT**

The contract will begin on July 1, 2024.

The contract will end on June 30, 2027.

The State will have the opportunity to renew the contract for two 1-year time extensions. The extensions will not be automatic.

### **1.16 GOVERNING LAW**

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

### **1.17 SITE VISIT**

If site visits are required, they will be scheduled before the submission of the proposal. Site visits will be made at the offeror's expense.

## **1.18 PRESENTATIONS/DEMONSTRATIONS**

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

## **1.19 DISCUSSIONS**

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.

## **1.20 NEGOTIATIONS**

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 component 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 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, 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, attached hereto as Section 3 of the RFP and by this reference incorporated herein.
- 2.2** The Contractor's services under this Agreement will start on July 1, 2024 and end on June 30, 2027, unless terminated sooner pursuant to the terms of the Agreement. The State will have the opportunity to renew the contract for two 1-year time extensions. The extensions will not be automatic.
- 2.3** The Contractor will not use State equipment, supplies, or facilities. 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 TOTAL CONTRACT AMOUNT is an amount not to exceed \$\_\_\_\_. The State will not pay Contractor's expenses as a separate item. Payment will be made pursuant to itemized invoices submitted with a signed state voucher. Payment will be made consistent with SDCL chapter 5-26.
- 2.5** The Contractor will 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 under this Agreement. 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, will obtain and maintain in force

insurance coverage of the types and with the limits as follows:

- A. **Commercial General Liability Insurance:**  
The Contractor will maintain occurrence based commercial general liability insurance or equivalent form with a limit of not less than \$1 million for each occurrence. If such insurance contains a general aggregate limit it will 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 million.
- C. **Business Automobile Liability Insurance:**  
The Contractor will maintain business automobile liability insurance or equivalent form with a limit of not less than \$1 million for each accident. Such insurance will include coverage for owned, hired, and non-owned vehicles.
- D. **Workers' Compensation Insurance:**  
The Contractor will procure and maintain workers' compensation and employers' liability insurance as required by South Dakota law.

Before beginning work under this Agreement, Contractor will furnish the State with properly executed Certificates of Insurance which will 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 will furnish copies of insurance policies if requested by the State.

- 2.7** While performing services under this Agreement, the Contractor is an independent contractor and not an officer, agent, or employee of the State of South Dakota.
- 2.8** The 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. The Contractor will report any such event to the State immediately upon discovery.
- 2.9** The Contractor's obligation under this section will 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. The Contractor's obligation to report will 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 will not excuse or satisfy any obligation of the Contractor to report any event to law enforcement or other entities under the requirements of any applicable law.
- 2.10** 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 of this Agreement, this Agreement may be terminated by the State at any time with or without notice. If termination for such a default is affected by the State, any payments due to the Contractor at the time of termination may be adjusted to cover any additional costs to the State because of the 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 the Contractor it is determined that the Contractor was not at fault, then the Contractor will be paid for eligible services rendered and expenses incurred up to the date of termination.
- 2.11** 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.

- 2.12** 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 will be expressly identified as a part of this Agreement and be signed by an authorized representative of each of the parties to this Agreement.
- 2.13** This Agreement will be governed by and construed in accordance with the laws of the State of South Dakota. Any lawsuit pertaining to or affecting this Agreement will be venued in Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota.
- 2.14** 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.
- 2.15** The Contractor may not use subcontractors to perform the services described in this Agreement without the express prior written consent of the State. 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 and will adopt such review and inspection procedures as are necessary to assure such compliance.
- 2.16** The 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 will 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.
- 2.17** 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.
- 2.18** By signing this Agreement, the Contractor certifies and agrees that it has not refused to transact business activities, have not terminated business activities, and have not taken other similar actions intended to limit its commercial relations, related to the subject matter of this Agreement, with a person or entity that is either the State of Israel, or a company doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel to do business, or doing business in the State of Israel, 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 terminate this Agreement. During the term of this Agreement, if the Contractor no longer complies with this certification, the Contractor agrees to provide immediate written notice to the State and agrees such noncompliance may be grounds for termination of this Agreement.
- 2.19** Pursuant to South Dakota Codified Law § 5-18A, by entering into this Agreement with the State of



South Dakota, the Contractor certifies and warrants that the Contractor is not a prohibited 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 Codified Law § 5-18A.

The Contractor agrees that if this certification is false, the State may terminate this Agreement with no further liability to the State. The Contractor further agrees to provide immediate written notice to the State if during the term of the contract it no longer complies with this certification, and the Contractor agrees such noncompliance may be grounds for contract termination and would be cause to suspend and debar a business under SDCL § 5-18D-12.

- 2.20** Pursuant to South Dakota Executive Order 2023-04, by entering into this Agreement with the State of South Dakota, the contract certifies and warrants that the Contract has not discriminated against a firearm-related entity, regardless of whether the subject matter of this Agreement is related to the discriminatory activity of the Contractor, as defined by South Dakota Executive Order 2023-04.

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

- 2.21** The Contractor (i) understands neither a state legislator nor a business in which a state legislator has an ownership interest may be directly or indirectly interested in any contract with the State that was authorized by any law passed during the term for which that legislator was elected, or within one year thereafter, and (ii) has read South Dakota Constitution Article 3, Section 12 and has had the opportunity to seek independent legal advice on the applicability of that provision to this Agreement. By signing this Agreement, the Contractor certifies that this Agreement is not made in violation of the South Dakota Constitution Article 3, Section 12.
- 2.22** Any notice or other communication required under this Agreement will be in writing and sent to the address set forth above. Notices will be given by and to \_\_\_\_\_ on behalf of the State, and by and to \_\_\_\_\_, on behalf of the Contractor, or such authorized designees as either party may from time to time designate in writing. Notices or communications to or between the parties will be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination will be sent by registered or certified mail, or, if personally delivered, when received by such party.
- 2.23** In the event that any court of competent jurisdiction will hold any provision of this Agreement unenforceable or invalid, such holding will not invalidate or render unenforceable any other provision of this Agreement.
- 2.24** 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 in this Agreement, this Agreement constitutes the entire agreement with respect to the subject matter.

### **3 SCOPE OF WORK**

- 3.1** The Offeror shall review the Department's current website, including available analytic data, and create a more efficient, intuitive, and user-friendly web experience. The new site must be mobile friendly and include a comprehensive search engine so users can easily locate the content they wish to find. Training on the customized content management system in the form of paper manuals or video is desired. Offerors are expected to work with the Department to design the website and draft/revise the content provided. The Department is also interested in analytics reporting and site performance review for the new site.

### 3.2 Scope of Components or Phases:

- A. Hold discovery sessions with staff from individual DPS agencies to determine the specific needs and functionality of their agency pages.
- B. Build the site.
- C. Build the content management system (if separate line item)
- D. Write/copy content in new site.
- E. Proof/edit content until final version is approved.
- F. Train staff on use of the content management system (in-person, virtually, provide training videos, etc.).
- G. Any other steps recommended by vendor prior to the launch date.
- H. Launch the new website.
- I. Provide assistance/support under any ongoing maintenance hours included in the contract.

- 3.3 The proposal should provide an option for the State to have the vendor host the website in their cloud environment or in the State's Azure Cloud environment.

### 3.4 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.

### 3.5 Single Sign-On Requirements

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

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

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

### 3.6 Onboarding/Provisioning Users

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

### 3.7 Interfaces and Integration

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

### 3.8 Solution Diagram

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

### 3.9 Web Content Accessibility Guideline

If applicable, the offeror's application is required to conform to the Web Content Accessibility Guidelines 2.0.

### 3.10 Any website must meet the Web standards listed in this RFP and as found in the following:

[https://www.sd.gov/bit?id=bit\\_standards\\_web](https://www.sd.gov/bit?id=bit_standards_web)  
[https://www.sd.gov/bit?id=bit\\_standards\\_vendor\\_client\\_sec\\_req](https://www.sd.gov/bit?id=bit_standards_vendor_client_sec_req)

### 3.11 The proposed Content Management System (CMS) cannot be WordPress or PHP-supported.

## 4 RESOURCES

The Bureau of Information and Telecommunications (BIT) is the state organization that provides IT services for the state.

Historically, the most successful projects are those that use the team approach. The team approach utilizes a combination of consultant staff, BIT staff, and Agency staff. Below is a description of how the team will be structured.

### 4.1 TEAM ORGANIZATION: Provide the following information.

#### 4.1.1 PROJECT ORGANIZATION CHART

List names, job titles (designate vacancies), and the city and state in which individual will work on this project.

#### 4.1.2 LIST OF ALL CONSULTANTS AND SUBCONTRACTORS

List all entities to be used for performance of the services described in this RFP. In the work plan, describe which responsibilities will be assigned to consultants or subcontractors and the city and state in which the consultants or subcontractors are located.

### 4.2 PROJECT STAFFING ROLES

#### Agency Project Sponsor

**Who:** This is an Agency Manager for whom the project is undertaken and who are the primary stake holder and the primary risk taker.

**Role:** Some of the duties performed by the Agency Project Sponsor are:

- Resolves resource and priority conflicts
- Approves the Project Charter and/or Plan
- Holds subordinate managers accountable for their performance
- Direct communication and reporting relationship with the Agency Project Manager.
- Chief advocate for the project.

- Keeps the team focused on appropriate goals
- Keeps the team updated with new information
- Holds the project team accountable planning and executing the project
- Holds the team accountable for delivering agreed-upon results

### **Development Team Project Manager**

**Who:** This person may be either a BIT employee or a consultant employee.

**Role:** Some of the duties performed by the Development Team Project Manager are:

- Provides day to day supervision of the employees of the development team
- In close daily contact with the Agency Project Manager to ensure that all requirements are fulfilled
- Able to advise the Agency Project Manager of cost/benefit as well as consequences of any changes in work direction

**Reports to:** Agency Project Manager. Also reports to the Project Steering Team if one exists.

### **Agency Project Manager**

**Who:** This person will typically be an Agency employee, appointed by the Project Sponsor. This could be a full-time job on large projects.

**Role:** Some of the duties performed by the Agency Project Manager are:

- Day to day oversight of the project
- Approves consultant payments based on contract/work order language
- Provides direction to Agency employees as well as the team

**Reports to:** The Agency Project Sponsor. This person must keep the Project Sponsor informed on a weekly basis regarding progress and status of the project. When issues arise, this person must be able to make recommendations to the team regarding amendments and changes to the deliverables, schedule or budget.

### **Project Security Lead**

**Who:** This person would be a consultant employee and must be identified by the consultant.

**Role:** The security lead shall certify in writing the security of each deliverable. The security lead will have overall responsibility for the security of the application development, management, and update process throughout the contract period.

**Reports to:** The Agency Project Sponsor as part of the project status meetings. When issues arise, this person must be able to make recommendations to the team regarding amendments and changes to the deliverables, schedule or budget.

### **Project Steering Team**

**Who:** This team consists of at least one member from each affected departmental area and may include an offeror representative.

**Role:** Some of the duties performed by the Project Steering Team:

- Oversee the project in terms of the contract and work order agreements. Specific items of oversight include:
  - What are the deliverables for his or her agency, and are they being met?

- Is the project on schedule? If not, what are the consequences? Should the project be put back on schedule and how will that be done?
- What expenditures have been made? Is the project on budget? If not, what are the circumstances surrounding it?
- Recommendation of approval of any scope changes, or any changes that affect cost and schedule based on cost benefit to the Project Owner

**Reports to:** Their Agency Manager.

**Authority:** Each Steering Team member should have authority to make decisions for their own departmental area.

#### **4.3 STAFF RESUMES AND REFERENCES**

Resumes and references of key personnel, key personnel are considered to be those who are accountable for the completion of one or more major deliverables, has the responsibility of any or all of the total project management, or is responsible for the completion of the project. Provide resume details for all key personnel, including any subcontractors' project leads, by listing the following in the order in which it appears.

- Name
- Title
- Contact Information (telephone number(s), e-mail address)
- Work Address
- Project Responsibilities (as they pertain to this project)
- Percentage of time designated to this project
- Brief listing of Work Experience in reverse chronological order from present to July 15, 2018 (only provide company name, job title(s)/position(s) held, date started, and date left each position, brief description of job duties, responsibilities, and significant accomplishments)
- RFP Project Experience
- Technical Background relative to this project
- Experience in Similar Projects
- Names of the Similar Projects they were involved in
- Role they played in the projects similar to this project
- Project Management Experience
- Technical Knowledge
- Education
- Relevant Certifications
- Three Professional References (name, telephone number, company name, relationship to employee)

#### **5 PROJECT DELIVERABLES/APPROACH/METHODOLOGY**

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

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

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

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

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

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

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

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

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

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

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

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

security scans by BIT.

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

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

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

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

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

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

If the offeror's solution requires accounts allowing access to State systems, then the offeror must indicate the number of the offeror's staff or subcontractors that will require access, the level of access needed, and if these accounts will be used for remote access. These individuals will be required to use Multi-Factor Authentication (MFA). The State's costs in providing these accounts will be a consideration when assessing the cost of the offeror's solution. If the offeror later requires accounts that exceed the number of accounts that was originally indicated, the costs of those accounts will be borne by the offeror and not passed onto the State. All State security policies can be found in the Information Technology Security Policy (ITSP) attached to this RFP. The offeror should review the State's security policies regarding

authorization, authentication, and, if relevant, remote access (See ITSP 230.67, 230.76, and 610.1). Use of Remote Access Devices (RAD) by contractors to access the State's system must be requested when an account is requested. The offeror should be aware that access accounts given to non-state employees, Non-State (NS) accounts, will be disabled if not used within 90 days. A NS account may be deleted after 30 days if it is not used.

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

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

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

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

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

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

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

## **6 FORMAT OF SUBMISSION**

All proposals should be prepared simply and economically and provide a direct, concise explanation of the offeror's proposal and qualifications. Elaborate brochures, sales literature and other presentations unnecessary to a complete and effective proposal are not desired.

Offerors are required to provide an electronic copy of their response. The electronic copy should be provided in MS WORD or in PDF format, except for the project plan, which must be in MS Project. The submission must be delivered as indicated in Section 1.6 of this document.



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. The offeror should respond to each point in the Scope of Work and Deliverables in the order they were presented.

Offerors and their agents (including subcontractors, employees, consultants, or anyone else acting on their behalf) must direct all questions or comments regarding the RFP or the evaluation to the buyer of record indicated on the first page of this RFP. Offerors and their agents may not contact any state employee other than the buyer of record regarding any of these matters during the solicitation and evaluation process. Inappropriate contacts are grounds for suspension and exclusion from specific procurements. Offerors and their agents who have questions regarding this matter should email the buyer of record at [DPSinfo@state.sd.us](mailto:DPSinfo@state.sd.us).

The offeror may be required to submit a copy of its most recent audited financial statements upon the State's request.

The proposal should be page numbered and should have an index or a table of contents referencing the appropriate page number. Each of the sections listed below should be tabbed.

Offerors are cautioned that use of the State Seal in any of their documents is illegal as per South Dakota Codified Law § 1-6-3.1. *Use of seal or facsimile without authorization prohibited--Violation as misdemeanor. No person may reproduce, duplicate, or otherwise use the official seal of the State of South Dakota, or its facsimile, adopted and described in §§ 1-6-1 and 1-6-2 for any for-profit, commercial purpose without specific authorization from the secretary of state. A violation of this section is a Class 1 misdemeanor.*

Proposals should be prepared using the following headings and, in the order that they are presented below. Please reference the section for details on what should be included in your proposal.

- Statement of Understanding of Project
- Deliverables
- Non-standard Software and/or Hardware
- Project Plan
- System Diagram (If not a separate document)
- Security and Vendor Questions (If not a separate document)
- Response to the State's contract terms
- Corporate Qualifications
- Project Experience
- Team Organization
- Staffing
- Costs (If not a separate document)

## **6.1 STATEMENT OF UNDERSTANDING OF PROJECT**

To demonstrate your comprehension of the project, the offeror should summarize their understanding of what the work is and what the work will entail. This should include, but not be limited to, the offeror's understanding of the purpose and scope of the project, critical success factors and potential problems related to the project, and the offeror's understanding of the deliverables. The offeror should include their specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements. This section should be limited to no more than two pages.

## 6.2 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. The State of South Dakota has a consolidated IT system. **Either** any references given should be from states with a consolidated IT system, to be acceptable **or** the reference should be a detailed explanation on how you will modify your work plan for a consolidated environment that you are unfamiliar with.
- S. Provide the reports of third-party security scans done at the end of the four projects you provided in your proposal response. If there are no audits of these projects then provide, unedited and un-redacted results of such security testing/scanning from third-party companies or tools that has been run within the past 90 days. The State will sign a non-disclosure

agreement, as needed, and redaction of these scan reports can be done within the limits of the State's open records law.

T. What is your Company's web site?

When providing references, the reference must include the following information:

- Name, address and telephone number of client/contracting agency and a representative of that agency who may be contacted for verification of all information submitted
- Dates of the service/contract
- A brief, written description of the specific prior services performed and requirements thereof

### **6.3 RELEVANT PROJECT EXPERIENCE**

Provide details about four recent projects that the offeror was awarded and then managed through to completion. Project examples should include sufficient detail so the agency fully understands the goal of the project; the dates (from start to finish) of the project; the offeror's scope of work for the project; the responsibilities of the offeror and subcontractors in the project; the complexity of the offeror's involvement in the project; deliverables provided by the offeror; the methodologies employed by the offeror; level and type of project management responsibilities of the offeror; changes that were made and request for changes that differed from the onset of the project; how changes to the project goals, offeror's scope of work, and deliverables were addressed or completed; price and cost data; quality of the work and the total of what the offeror accomplished in the project.

- A. Client/Company Name
- B. Client Company Address, including City, State and Zip Code
- C. Client/Company Contacts(s)
  - Name
  - Title
  - Telephone Number
  - E-mail address
  - Fax Number
- D. Project Start Date
- E. Project Completion Date
- F. Project Description and Goals
- G. Offeror's Role in Project
- H. Offeror's responsibilities
- I. Offeror's Accomplishments
- J. Description of How Project Was Managed
- K. Description of Price and Cost Data from Project
- L. Description of special project constraints, if applicable
- M. Description of your ability and proven history in handling special project constraints
- N. Description of All Changes to the Original Plan or Contract That Were Requested
- O. Description of All Changes to the Original Plan or Contract That Offeror Completed
- P. Description of How Change Requests Were Addressed or Completed by Offeror
- Q. Was Project Completed in a Timeframe That Was According to the Original Plan or Contract? (If "No", provide explanation)
- R. Was Project Completed Within Original Proposed Budget? (If "No" provide explanation)

- S. Was there any Litigation or Adverse Contract Action regarding Contract Performance? (If “Yes” provide explanation)
- T. Feedback on Offeror’s Work by Company/Client
- U. Offeror’s Statement of Permission for the Department to Contact the Client/Company and for the Client’s/Company’s Contract(s) to Release Information to the Department

#### **6.4 PROJECT PLAN**

Provide a project plan that indicates how you will complete the required deliverables and services and addresses the following:

- Proposed project management techniques
- Number of offeror’s staff needed
- Tasks to be performed (within phase as applicable)
- Number of hours each task will require
- Deliverables created by each task
- Dates by which each task will be completed (dates should be indicated in terms of elapsed time from project inception)
- Resources assigned to each task
- Required state agency support
- Show task dependencies
- Training (if applicable)

Microsoft Project is the standard scheduling tool for the State of South Dakota. The schedule should be a separate document, provided in Microsoft Excel, and submitted as an attachment to your proposal.

If, as part of this project, the offeror plans to set up or configure the software or hardware and plans to do this outside of South Dakota, even in part, then the offeror needs to provide a complete and detailed project plan on how the offeror plans on migrating to the State’s site. Failure to do this is sufficient grounds to disregard the submission, as it demonstrates that the offeror fundamentally does not understand the project. Providing a work plan for the steps above that is complete and detailed may be sufficient.

#### **6.5 DELIVERABLES**

This section should constitute the major portion of the work to be performed. Provide a complete narrative detailing the assessment of the work to be performed, approach and methods to provide the requirements of this RFP, the offeror’s ability to fulfill the requirements of this RFP, the offeror’s approach, the resources necessary to fulfill the requirements, project management techniques, specialized services, availability to the project locale, familiarity with the project locale and a description of any options or alternatives proposed. This should demonstrate that the offeror understands the desired overall performance expectations. This response should identify each requirement being addressed as enumerated in section 8. If you have an alternative methodology or deliverables you would like to propose, please include a detailed description of the alternative methodology or deliverables and how they will meet or exceed the essential requirements of the methodology and deliverables described in Section 6.

#### **6.6 NON-STANDARD HARDWARE AND SOFTWARE**

State standard hardware and software should be utilized unless there is a reason not to. If your proposal will use non-standard hardware or software, you must first obtain State approval. If your proposal recommends using non-standard hardware or software, the proposal should very clearly indicate what non-standard hardware or software is being proposed and why it is necessary to use

non-standard hardware or software to complete the project requirements. The use of non-standard hardware or software requires use of the State's New Product Process. This process can be found through the Standards' page and must be performed by State employees. The costs of such non-standard hardware or software should be reflected in your cost proposal. The work plan should also account for the time needed to complete the New Product Process. See [https://bit.sd.gov/bit?id=bit\\_standards\\_overview](https://bit.sd.gov/bit?id=bit_standards_overview), for lists of the State's standards. The proposal should also include a link to your hardware and software specifications.

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

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

## 6.7 BACKGROUND CHECKS

The offeror must include the following statement in its proposal:

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

## 7 COST PROPOSAL

Cost will be evaluated independently from the technical proposal. Offerors may submit multiple cost proposals. All costs related to the provision of the required services must be included in each cost proposal offered.

The offeror must submit a statement in the Proposal that attests the offeror's willingness and ability to perform the work described in this RFP for the price being offered.

### 7.1 STAFFING

Name	Role	Total Hours on Project	Total Hours on Site	Hourly Rate	Total
				Total:	

## 7.2 TRAVEL AND EXPENDITURE TABLE

Name	Method of Travel	Cost per trip	Number of Trips	Total Cost
			Total:	

Name	Lodging Cost per night	Number of Nights	Lodging Cost	Per diem	Number of Days	Per diem Cost	Total Cost
Totals:							

NOTE: The State asks that vendors accept state per diem. Lodging and per diem rates can be found at <https://bhr.sd.gov/files/travelrates.pdf>.

## 7.3 OTHER COSTS

Show any other costs such as: software, hardware, ongoing costs, etc.

	One Time	Year 1	Year 2	Year 3	Totals
Hardware					
Software					
Maintenance					
License Fees					
Training					
Other...					
Totals					

## 7.4 ADDITIONAL WORK

The offeror may be expected to perform additional work as required by any of the State signatories to a contract. This work can be made a requirement by the State for allowing the application to go

into production. This additional work will not be considered a project change chargeable to the State if it is for reasons of correcting security deficiencies, meeting the functional requirements established for the application, unsupported third-party technologies or excessive resource consumption. The cost for additional work should be included in your proposal.

## **8 PROPOSAL EVALUATION AND AWARD PROCESS**

- 8.1** 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:
- 8.1.1** Specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements;
  - 8.1.2** Resources available to perform the work, including any specialized services, within the specified time limits for the project;
  - 8.1.3** Record of past performance, including price and cost data from previous projects, quality of work, ability to meet schedules, cost control, and contract administration;
  - 8.1.4** Availability to the project locale;
  - 8.1.5** Familiarity with the project locale;
  - 8.1.6** Proposed project management techniques; and
  - 8.1.7** Ability and proven history in handling special project constraints
- 8.2** Experience and reliability of the offeror's organization are considered subjectively in the evaluation process. Therefore, the offeror is advised to submit any information which documents successful and reliable experience in past performances, especially those performances related to the requirements of this RFP.
- 8.3** The qualifications of the personnel proposed by the offeror to perform the requirements of this RFP, whether from the offeror's organization or from a proposed subcontractor, will be subjectively evaluated. Therefore, the offeror should submit detailed information related to the experience and qualifications, including education and training, of proposed personnel.
- 8.4** 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.
- 8.5 Award.** 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.
- 8.5.1** 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 offeror. The agency may then negotiate with the next highest ranked offeror.
  - 8.5.2** The negotiation process may continue through successive offerors, according to agency ranking, until an agreement is reached, or the agency terminates the contracting process.

## **9 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 an offeror. Best and final offers may not be necessary if the State is satisfied with the proposals received.

If best and final offers are sought, the State will document which offerors 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 an offeror does not submit a best and final offer or a notice of withdrawal, the offeror's previous proposal will be considered that offeror's best and final proposal. After best and final offers are received, final evaluations will be conducted.



## 10 SCANNING

The offeror acknowledges that the State will conduct a security and vulnerability scan as part of the review of the offeror's RFP. This scan will not include a penetration test. The State will use commercially available, industry standard tools to scan a non-production environment with non-production data at mutually agreeable times.

The offeror should fill in the information below and sign the form. The offeror's employee signing this form must have the authority to allow the State to do a security scan. If no security contact is given the State will assume that the State can scan at any time. **At the state's option, any RFP response that does not include a completed and signed form may be dropped from consideration. If there is State data protected by federal or state law or regulation or industry standard involved, the State is more likely to consider a security scan necessary for an RFP to be considered.** Except for State staff, the State will only provide scan information to the offeror's security contact. At the State's option, the State will conduct the scan at a location named by the offeror. The offeror can only request, not require, naming the scanning location. The State may consider a full scan report from industry standard Web Application Vulnerability scanning tools (ex. Invicti, Burp Suite, Nmap, Qualys, Nessus, etc...) as satisfying the scanning requirement. Executive Summaries, penetration test methodology/vulnerability summary reports, and/or SOC I/SOC II are not considered as sufficient replacements for a vulnerability scan. If required, the State will sign a non-disclosure agreement before scanning or receiving the full security assessment.

Offeror's name: \_\_\_\_\_

Offeror's security contact's name: \_\_\_\_\_

Security contact's phone number: \_\_\_\_\_

Security contact's email address: \_\_\_\_\_

Web address URL or Product Name \_\_\_\_\_. The State will contact the security contact to arrange for a test log for scanning.

Offeror's employee acknowledging the right to scan:

Name (Print): \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Signature: \_\_\_\_\_

## Appendix A

### **Bureau of Information and Telecommunications Required IT Contract Terms and Conditions**

**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 \$\_\_\_\_\_ 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. Software Functionality and Replacement**

The software licensed by the Vendor to the State under this Agreement will provide the functionality as described in the software documentation, which the Vendor agrees to provide to the State prior to or upon the execution of

this Agreement.

The Vendor agrees that:

- A. If, in the opinion of the State, the Vendor reduces or replaces the functionality contained in the licensed product and provides this functionality as a separate or renamed product, the State will be entitled to license such software product at no additional license or maintenance fee.
- B. If, in the opinion of the State, the Vendor releases an option, future product, purchasable product or other release that has substantially the same functionality as the software product licensed to the State, and it ceases to provide maintenance for the older software product, the State will have the option to exchange licenses for such replacement product or function at no additional charge. This includes situations where the Vendor discontinues the licensed product and recommends movement to a new product as a replacement option regardless of any additional functionality the replacement product may have over the licensed product.

## **Section VI. Service Bureau**

Consistent with use limitations specified in the Agreement, the State may use the product to provide services to the various branches and constitutional offices of the State of South Dakota as well as county and city governments, tribal governments, and school districts. The State will not be considered a service bureau while providing these services and no additional fees may be charged unless agreed to in writing by the State.

## **Section VII. Federal Intellectual Property Bankruptcy Protection Act**

The Parties agree that the State will be entitled to all rights and benefits of the Federal Intellectual Property Bankruptcy Protection Act, Public Law 100-506, codified at 11 U.S.C. 365(n), and any amendments thereto. The State also maintains its termination privileges if the Vendor enters bankruptcy.

## **Section VIII. 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 IX. 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 X. 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 XI. 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 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. 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 XIX. 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 XX. 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 XXI. Security of Code**

Any code written or developed pursuant to the terms of this Agreement must comply with the security requirements of this Agreement.

#### **Section XXII. 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](https://bit.sd.gov/bit?id=bit_standards_overview).

#### **Section XXIII. Acceptable Programming Languages**



All applications covered by this Agreement will be written in C#, and use ASP.NET, Model View and Controller (MVC), Universal Windows Platform (UWP), or Windows Presentation Foundation (WPF).

## **Section XXIV. 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 XXV. 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.
- C. All members of the development team have been successfully trained in secure programming techniques.
- D. A source code control system will be used that authenticates and logs the team member associated with all changes to the software baseline and all related configuration and build files.
- E. State access to the source code will be allowed to ensure State security standards, policies, and best practices which can be found at [https://bit.sd.gov/bit?id=bit\\_standards\\_overview](https://bit.sd.gov/bit?id=bit_standards_overview).
- F. The Vendor will fully support and maintain the Vendor's application on platforms and code bases (including but not limited to: operating systems, hypervisors, web presentation layers, communication protocols, security products, report writers, and any other technologies on which the application depends) that are still being supported, maintained, and patched by the applicable third parties owning them. The Vendor may not withhold support from the State for this application nor charge the State additional fees as a result of the State moving the Vendor's application to a new release of third-party technology if:
  - 1. The previous version of the third-party code base or platform is no longer being maintained, patched, and supported; and
  - 2. The new version to which the State moved the application is actively maintained, patched, and supported.

If there are multiple versions of the applicable code base or platform(s) supported by the third party in question,

the Vendor may limit its support and maintenance to any of the applicable third-party code bases or platforms.

If a code base or platform on which the Vendor's application depends is no longer supported, maintained, or patched by a qualified third party the Vendor commits to migrate its application from that code base or platform to one that is supported, maintained, and patched after the State has performed a risk assessment using industry standard tools and methods. Failure on the part of the Vendor to work in good faith with the State to secure a timely move to supported, maintained, and patched technology will allow the State to cancel this Agreement without penalty.

## **Section XXVI. 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 XXVII. Secure Product Development**

By signing this Agreement, the Vendor agrees to provide the following information to the State:

- A. Name of the person responsible for certifying that all deliverables are secure.
- B. Documentation detailing the Vendor's version upgrading process.
- C. Notification process for application patches and updates.
- D. List of tools used in the software development environment used to verify secure coding.
- E. Based on a risk assessment, provide the State the secure configuration guidelines, specifications and requirements that describe security relevant configuration options and their implications for the overall security of the software. The guidelines, specifications and requirements must include descriptions of dependencies on the supporting platform, including operating system, web server, application server and how they should be configured for security. The default configuration of the software shall be secure.

At the State's discretion the State will discuss the security controls used by the State with the Vendor upon the Vendor signing a non-disclosure agreement.

## **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. License Agreements**

The Vendor warrants that it has provided to the State and incorporated into this Agreement all license agreements, End User License Agreements (EULAs), and terms of use regarding its software or any software incorporated into its software before execution of this Agreement. Failure to provide all such license agreements, EULAs, and terms of use will be a breach of this Agreement at the option of the State. The parties agree that neither the State nor its end users will be bound by the terms of any such agreements not timely provided pursuant to this paragraph and incorporated into this Agreement. Any changes to the terms of this Agreement or any additions or subtractions must first be agreed to by both parties in writing before they go into effect. This paragraph will control and supersede the language of any such agreements to the contrary.

## **Section XXXVII. 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, and
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 XXXVIII. 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 XXXIX. 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 XL. 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 XLI. 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 XLII. Vendor’s Software Licenses**

The Vendor must disclose to the State any license for all third-party software and libraries used by the Vendor’s product(s) covered under this Agreement if the State will not be the license holder. The Vendor is required to

provide a copy of all licenses for the third-party software and libraries to the State. No additional software and libraries may be added to the project after this Agreement is signed without notifying the State and providing the licenses to the software and libraries. Open-source software and libraries are also covered by this clause. Any validation of any license used by the Vendor to fulfil the Vendor's commitments agreed to in this Agreement is the responsibility of the Vendor, not the State.

### **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, Nuctech, 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 not copy, disclose, retain, or use State Data for any purpose other than to fulfill its obligations under this Agreement.
- B. 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. 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, Nuctech, 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 LVI. 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 before this data can be accessed. The Vendor's MFA, at a minimum must adhere to the requirements of *Level 2 Authentication Assurance for MFA* as defined in NIST 800-63.



## Appendix B – Security and Vendor Questions

### Basic Vendor Information

Vendor Legal Name:

Vendor Address:

### Directions

**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. Your response to the questions allows BIT an opportunity to review the security of your product, and helps BIT make an informed decision and recommendation regarding your technology or service. 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.

The State understands that some of the information you may provide when answering the questions is considered confidential or proprietary. Please mark which answers you deem to be confidential/proprietary information. Access to this confidential information will be limited to those state employees who have a need to know. In addition, the State will maintain the confidentiality of the marked information, and the marked information may be exempt from disclosure to the public per the State’s Open Records Laws.

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 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 Contact.

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?	<input type="checkbox"/> State Hosted On-prem (dedicated VM/infrastructure) <input type="checkbox"/> State Cloud Provider (PaaS Solution) <input type="checkbox"/> Vendor Hosted <input type="checkbox"/> Other: (Please state)
2	DC DEV TEL	What type of access is required by vendor or proposed solution to state hosted or external resources?	<input type="checkbox"/> Not Required <input type="checkbox"/> VPN <input type="checkbox"/> API <input type="checkbox"/> SFTP <input type="checkbox"/> Other: (Please state)
3	DC	What type of access is required by vendor to maintain and support the solution?	<input type="checkbox"/> Not Required <input type="checkbox"/> Citrix (For On-prem) <input type="checkbox"/> State Cloud Access <input type="checkbox"/> Other: (Please state)



<b>4</b>	TEL	If an on-prem solution, which of the following will apply?	<input type="checkbox"/> IoT Hardware <input type="checkbox"/> Non-Windows or non-domain joined solution <input type="checkbox"/> Windows-based domain joined hardware <input type="checkbox"/> Other: (Please state)
<b>5</b>	DC TEL	Does your proposed solution include/require additional devices connected to the application for activities such as scanning or printing?	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>6</b>	DC	Does the proposed solution include the use of email?	<input type="checkbox"/> Yes <input type="checkbox"/> No If "Yes", please describe how email will be used:
<b>7</b>	POC TEL	Will there be any desktop software installs, policies, or software required on state managed computers as part of this product?	<input type="checkbox"/> Yes <input type="checkbox"/> No If "Yes", please define:
<b>8</b>	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:
<b>9</b>	POC	Will any hardware or peripherals need to be attached to or added to state managed computers?	<input type="checkbox"/> Yes <input type="checkbox"/> No If "Yes", please define:
<b>10</b>	POC	Will any browser plugins be required to install, access, or use this product?	<input type="checkbox"/> Yes <input type="checkbox"/> No If "Yes", please define:
<b>11</b>	POC	Will any products that connect or interact with a state managed computer or network be required as part of this product or project?	<input type="checkbox"/> Yes <input type="checkbox"/> No If "Yes", please define:
<b>12</b>	POC	Will any Bluetooth or RF frequency devices be required as part of this product or project?	<input type="checkbox"/> Yes <input type="checkbox"/> No If "Yes", please define:
<b>13</b>	POC	What operating system is the software/hardware compatible with?	<input type="checkbox"/> Microsoft Windows 10 <input type="checkbox"/> Microsoft Windows 11 <input type="checkbox"/> Other (please specify): <input type="checkbox"/> Not Applicable
<b>14</b>	POC	For Vendor Hosted solutions, where are your data centers located (Please include locations for disaster recovery)?	Please provide locations:

**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 x	Does the solution require user authentication, and does that authentication solution support OpenID Connect or OAUTH2 to provide single sign-on? Please explain the authentication protocol(s) available to meet the State's single sign-on requirements and how that is implemented with one or more identity providers.					
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? If "Yes" please describe the encryption used (e.g. SHA256).					
A6	DC TEL x	<p>The protection of the State's system and data is of utmost importance. Web Application Vulnerability Scans must be done if:</p> <ul style="list-style-type: none"> <li>• An application will be placed on the State's system.</li> <li>• The State's system connects to another system.</li> <li>• The contractor hosts State data.</li> <li>• The contractor has another party host State data the State will want to scan that party.</li> </ul> <p><b><u>The State would want to scan a test system; not a production system and will not do penetration testing.</u></b> The scanning will be done with industry standard tools. Scanning would also take place annually as well as when there are code changes. Will you allow the State to scan a test system? If no, please explain or provide an alternative option to ensure protection of the State's system and data.</p>					
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)?					

<b>A10</b>	DEV	Are there any additional components or configurations required outside of the base product to meet the State's security needs?				
<b>A11</b>	TEL	What threat assumptions were made, if any, when designing protections for the software and information assets processed?				
<b>A12</b>	TEL	How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used?				
<b>A13</b>	TEL	What security criteria, if any, are considered when selecting third party suppliers?				
<b>A14</b>	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?				
<b>A15</b>	TEL	Has the software been evaluated against the Common Criteria, FIPS 140-3, 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.				
<b>A16</b>	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?				
<b>A17</b>	DC TEL x	Has the product undergone any vulnerability 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?				
<b>A18</b>	DC	Does your company have an executive-level officer responsible for the security of your company's software products and/or processes?				
<b>A19</b>	DC	How are software security requirements developed?				
<b>A20</b>	DC	What risk management measures are used during the software's design to mitigate risks posed by use of third-party components?				
<b>A21</b>	DC	What is your background check policy and procedure? Are your background checks fingerprint based? If required, would you be willing to undergo fingerprint-based background checks?				
<b>A22</b>	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.				
<b>A23</b>	TEL	What are the policies and procedures used to protect sensitive information from unauthorized access? How are the policies enforced?				
<b>A24</b>	DC TEL	Do you have an automated Security Information and Event Management system?				
<b>A25</b>	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:				
<b>A26</b>	DC	How are security logs and audit trails protected from tampering or modification? Are log files consolidated to single servers?				
<b>A27</b>	DEV	a. Are security specific regression tests performed during the development process?				
		b. If yes, how frequently are the tests performed?				
<b>A28</b>	TEL	What type of firewalls (or application gateways) do you use? How are they monitored/managed?				
<b>A29</b>	TEL	What type of Intrusion Detection System/Intrusion Protection Systems (IDS/IPS) do you use? How are they monitored/managed?				
<b>A30</b>	DC TEL	What are your procedures for intrusion detection, incident response, and incident investigation and escalation?				
<b>A31</b>	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)?				
<b>A32</b>	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?				

<b>A33</b>	POC	Will this system provide the capability to track data entry/access by the person, date, and time?				
<b>A34</b>	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.				
<b>A35</b>	DC	a. Do you have a SOC 2 or ISO 27001 audit report?				
		b. Is the audit performed annually?				
		c. When was the last audit performed?				
		d. If it is SOC 2 audit report, does it cover all 5 of the trust principles?				
		e. If it is a SOC 2 audit report, what level is it?				
		f. Does the audit include cloud service providers?				
		g. Has the auditor always been able to attest to an acceptable audit result?				
		h. Will you provide a copy of your latest SOC 2 or ISO 27001 audit report upon request? A redacted version is acceptable.				
<b>A36</b>	DC	Do you or your cloud service provider have any other security certification beside SOC 2 or ISO 27001, for example, FedRAMP or HITRUST?				
<b>A37</b>	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?				
<b>A38</b>	DC	Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all registry settings?				
<b>A39</b>	DC	What are your policies and procedures for hardening servers?				
<b>A40</b>	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 federal government's Entity List?				
<b>A41</b>	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: <ul style="list-style-type: none"> <li>• Security for their I/T systems;</li> <li>• Staff vetting;</li> <li>• Staff security training?</li> </ul>				
		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?				

<b>B11</b>	DC TEL	Do you use Content Threat Removal to extract and transform data?				
<b>B12</b>	DC TEL	Does your company have an endpoint detection and response policy?				
<b>B13</b>	DC TEL	Does your company have any real-time security auditing processes?				
<b>B14</b>	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?				
<b>B15</b>	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?				
<b>B16</b>	DC TEL	What anti-malware product(s) do you use?				
<b>B17</b>	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?				
<b>B18</b>	DC TEL	Have you ever had a data breach? If so, provide information on the breach.				
<b>B19</b>	POC	Is there a strategy for mitigating unplanned disruptions and what is it?				
<b>B20</b>	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?				
<b>B21</b>	POC	Will the State of South Dakota own the data created in your hosting environment?				
<b>B22</b>	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)?				

<b>D16</b>	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?				
<b>D17</b>	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?				
<b>D18</b>	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?				
<b>D19</b>	DC	What are your procedures and policies for handling and destroying sensitive data on electronic and printed media?				
<b>D20</b>	DC TEL	How is endpoint protection done? For example, is virus prevention used and how are detection, correction, and updates handled?				
<b>D21</b>	DC TEL	Do you perform regular reviews of system and network logs for security issues?				
<b>D22</b>	DC	Do you provide security performance measures to the customer at regular intervals?				
<b>D23</b>	DC POC	What technical, installation, and user documentation do you provide to the State? Is the documentation electronically available and can it be printed?				
<b>D24</b>	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?				
<b>D25</b>	DC DEV POC TEL	Will the implementation plan include performance testing?				
<b>D26</b>	DEV POC	Will there be documented test cases for future releases including any customizations done for the State of South Dakota?				
<b>D27</b>	DEV POC	If the State of South Dakota will gain ownership of the software, does the proposal include a knowledge transfer plan?				
<b>D28</b>	DEV POC	Has your company ever conducted a project where your product was load tested?				
<b>D29</b>	DC	Please explain the pedigree of the software. Include in your answer who are the people, organization, and processes that created the software.				
<b>D30</b>	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.				

<b>D31</b>	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? <b>Provide a brief explanation.</b> Will the supplier indemnify the acquirer from these issues in the license agreement? <b>Provide a brief explanation.</b>				
<b>D32</b>	DEV	Summarize the processes (e.g., ISO 9000, CMMi), methods, tools (e.g., IDEs, compilers), techniques, etc. used to produce and transform the software.				
<b>D33</b>	DEV	a. Does the software contain third-party developed components?				
		b. If yes, are those components scanned by a static code analysis tool?				
<b>D34</b>	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?				
<b>D35</b>	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.				
<b>D36</b>	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.				
<b>D37</b>	DC TEL	How are trouble tickets submitted? How are support issues, specifically those that are security-related escalated?				
<b>D38</b>	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.				
<b>D39</b>	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?				
<b>D40</b>	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?				
<b>D41</b>	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?				
<b>D42</b>	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.
<b>E1</b>	DEV POC x	What are the development technologies used for this system?				If marked yes, indicate version.
		ASP.Net				
		VB.Net				
		C#.Net				
		.NET Framework				
		Java/JSP				
		MS SQL				
		Other				
<b>E2</b>	DC TEL	Is this a browser-based user interface?				
<b>E3</b>	DEV POC	Will the system have any workflow requirements?				
<b>E4</b>	DC	Can the system be implemented via Citrix?				
<b>E5</b>	DC	Will the system print to a Citrix compatible networked printer?				
<b>E6</b>	TEL	If your application does not run under the latest Microsoft operating system, what is your process for updating the application?				
<b>E7</b>	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.				
<b>E8</b>	TEL x	Will your system use Adobe Air, Adobe Flash, Adobe ColdFusion, Apache Flex, Microsoft Silverlight, PHP, Perl, Magento, or QuickTime? If yes, explain?				
<b>E9</b>	DEV	To connect to other applications or data, will the State be required to develop custom interfaces?				
<b>E10</b>	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?				
<b>E11</b>	DEV POC	Has your company ever integrated this product with an enterprise service bus to exchange data between diverse computing platforms?				
<b>E12</b>	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).				
<b>E13</b>	DEV	What coding and/or API standards are used during development of the software?				
<b>E14</b>	DEV	Does the software use closed-source Application Programming Interfaces (APIs) that have undocumented functions?				
<b>E15</b>	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?				
<b>E16</b>	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?				
<b>E17</b>	DEV	What percentage of code coverage does your testing provide?				
<b>E18</b>	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?				
<b>E19</b>	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?				
<b>E20</b>	DC	Explain how and where the software validates (e.g., filter with whitelisting) inputs from untrusted sources before being used.				
<b>E21</b>	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?				
<b>E22</b>	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)?				
<b>E23</b>	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?				
<b>E24</b>	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 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.
<b>F1</b>	DC	Will the system infrastructure have a special backup requirement?				
<b>F2</b>	DC	Will the system infrastructure have any processes that require scheduling?				
<b>F3</b>	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?				
<b>F4</b>	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?				
<b>F5</b>	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?				
<b>F6</b>	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.				
<b>F7</b>	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.				
<b>F8</b>	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.				
<b>F9</b>	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.				
<b>F10</b>	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.				
<b>F11</b>	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.				
<b>F12</b>	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?				
<b>F13</b>	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.				
<b>F14</b>	POC x	List any hardware or software you propose to use that is not State standard, the standards can be found at: <a href="https://bit.sd.gov/bit?id=bit_standards_overview">https://bit.sd.gov/bit?id=bit_standards_overview</a> .				
<b>F15</b>	DC	Will your application require a dedicated environment?				
<b>F16</b>	DEV POC	Will the system provide an archival solution? If not, is the State expected to develop a customized archival solution?				
<b>F17</b>	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.				
<b>F18</b>	DC	Can the system be integrated with our enterprise Active Directory to ensure access is controlled?				
<b>F19</b>	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?				
<b>F20</b>	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. Windows Defender				
<b>F21</b>	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?				
<b>F22</b>	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?				
<b>F23</b>	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?				
<b>F24</b>	DC TEL	What physical access do you require to work on hardware?				
<b>F25</b>	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?				
<b>G14</b>	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?				
<b>G15</b>	DC	Are any of the professional services you plan to provide located outside the United States (e.g., help desk or transcription services)?				
<b>G16</b>	DC	Is the controlling share (51%+) of your company owned by one or more non-U.S. entities?				
<b>G17</b>	DC	What are your customer confidentiality policies? How are they enforced?				
<b>G18</b>	DC POC x	Will this application now or possibly in the future share PHI with other entities on other networks, be sold to another party, or be accessed by anyone outside the US?				
<b>G19</b>	DC	If the product is hosted at the State, will there be a request to include an application to monitor license compliance?				
<b>G20</b>	DC POC	Is telephone assistance available for both installation and use? If yes, are there any additional charges?				
<b>G21</b>	DC TEL	What do you see as the most important security threats your industry faces?				