

STATE OF SOUTH DAKOTA
OFFICE OF PROCUREMENT MANAGEMENT
523 EAST CAPITOL AVENUE
PIERRE, SOUTH DAKOTA 57501-3182

Request for Proposal for Construction Management System

PROPOSALS ARE DUE NO LATER THAN 5:00 PM CDT February 16, 2024

RFP #: 24RFP9741

BUYER: Damon Zeltinger

Email:
Damon.zeltinger@state.sd.us

READ CAREFULLY

OFFEROR INFORMATION

FIRM NAME: _____ AUTHORIZED SIGNATURE: _____

ADDRESS: _____ TYPE OR PRINT NAME: _____

CITY/STATE: _____ TELEPHONE #: _____

ZIP (9 DIGIT): _____ FAX #: _____

FEDERAL TAX ID#: _____ EMAIL: _____

PRIMARY CONTACT INFORMATION

NAME: _____ TELEPHONE #: _____

FAX #: _____ EMAIL: _____

TABLE OF CONTENTS

PRIMARY CONTACT INFORMATION	1
INSTRUCTIONS TO OFFERORS	3
1. GENERAL INFORMATION	3
2. COMPANY QUALIFICATIONS	5
3. PROPOSAL SUBMISSION	6
4. PROPOSAL FORMAT	7
5. SCOPE OF WORK	8
6. PROPOSAL EVALUATION AND AWARD	16
7. STANDARD CONTRACT TERMS AND CONDITIONS.....	20
8. PROJECT DELIVERABLES/APPROACH/METHODOLOGY.....	23
9. NON-STANDARD HARDWARE AND SOFTWARE.....	26
10. BACKGROUND CHECKS	26

INSTRUCTIONS TO OFFERORSA

1. GENERAL INFORMATION

1.1. PURPOSE OF REQUEST FOR PROPOSAL (RFP)

The State of South Dakota Department of Transportation (SDDOT) is issuing this Request for Proposal to select a qualified Contractor to provide a Commercial Off-the-Shelf (COTS) Construction Management System (CMS) and implementation services utilizing a Software as a Service (SaaS) model meeting the requirements defined in this RFP. Any contract resulting from this RFP is not exclusive and does not preclude the purchase of similar services from other sources.

A two-year contract will be issued for implementation of the software and a five-year commitment to subscription services, effective upon the date of fully executed contract and Notice to Proceed with the selected vendor. The State reserves the right, when circumstances require, to extend the period of this contract beyond the termination date for a period not to exceed 180 days if mutually agreeable to the Contractor and the State of South Dakota.

1.2. ISSUING OFFICE AND RFP REFERENCE NUMBER

The Operations Support Office is the issuing office for this document and all addenda relating to it, on behalf of SDDOT. The reference number for the transaction is RFP #24RFP9741. This number must be referred to in all proposals, correspondence, and documentation relating to the RFP.

1.3. SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)

RFP Release	January 9, 2024
Mandatory Preproposal Conference	January 16, 2024, 3:00-4:30pm Central Time
Deadline to submit questions	January 26, 2024
Official responses to questions posted	February 6, 2024
Proposals due	February 16, 2024
Notification of shortlisted vendors	March 1, 2024
BIT Short-Listed Vendor Interviews	March 6-7, 2024, and March 13-14, 2024
Conduct vendor demos	April 1-19, 2024
Cost proposals due	April 26, 2024, 5:00 p.m. Central Time ¹
Finalize selection and notice of award	May 3, 2024

¹ Cost proposals are due from short-listed vendors one week following their demonstration

1.4. Mandatory Preproposal Conference Information

Mandatory preproposal conference to be conducted remotely via Microsoft Teams. Meeting information is as follows:

https://teams.microsoft.com/l/meetup-join/19%3ameeting_NzA4ZTRmNjAtMmYzNC00MDUzLThiODYtZmlxZmVINWNkNGUz%40thead.v2/0?context=%7b%22Tid%22%3a%2270af547c-69ab-416d-b4a6-543b5ce52b99%22%2c%22Oid%22%3a%22de140c6a-20e1-4047-9a9f-456c43119eda%22%7d%3e

Meeting ID: 234 293 466 334 Passcode: 9qtUXt

Join with a video conferencing device teams@ddn.sd.gov<mailto:teams@ddn.sd.gov>
Video Conference ID: 118 116 043 0

Alternate VTC instructions<<https://confpool.ddn.sd.gov/teams/?conf=1181160430&ivr=teams&d=ddn.sd.gov&w>>

Or call in (audio only) +1 605-679-7263,,504521145#<tel:+16056797263,,504521145#>
United States, Sioux Falls Phone Conference ID: 504 521 145#

1.5. GOVERNING LAW

Venue for all legal action regarding or arising out of the transaction covered herein shall be solely in the State of South Dakota. The laws of South Dakota shall govern this transaction.

1.6. BIT 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 C along with any additional contract terms as negotiated by the parties. As part of the negotiation process the contract terms listed in Appendix C 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. 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.

2. COMPANY QUALIFICATIONS

- 2.1. By signing and submitting this proposal, the Offeror certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded by any federal department or agency from participation in transactions involving the use of federal funds. Where the Offeror is unable to certify to any of the statements in this certification, the bidder must attach an explanation to their offer.
- 2.2. No proposal will be accepted from and no contract will be awarded to any person, firm, or corporation that is in arrears upon any obligations to the State of South Dakota or that is otherwise deemed irresponsible or unreliable by the State Of South Dakota.
- 2.3. The Offeror may be required to submit a copy of their most recent audited financial statements upon the State's request.
- 2.4. 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.

2.5. CERTIFICATION RELATING TO 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 an entity, regardless of its principal place of business, that is ultimately owned or controlled, directly or indirectly, by a foreign national, a foreign parent entity, or foreign government from China, Iran, North Korea, Russia, Cuba, or Venezuela, as defined by SDCL 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.

2.6. RESTRICTION OF BOYCOTT OF ISRAEL

Contractors, vendors, suppliers, or subcontractors with five (5) or more employees that propose to enter into a contract with the State of South Dakota involving 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, certify and agree that the following information is correct:

The bidder or Offeror, in preparing its response or offer or in considering proposals submitted from qualified, potential vendors, suppliers, and subcontractors, or in the solicitation, selection, or commercial treatment of any vendor, supplier, or subcontractor, has not refused to transact business activities, has not terminated business activities, and has not taken other similar actions intended to limit its commercial relations, related to the subject matter of the bid or offer, with a person or entity on the basis of Israeli national origin, or residence or incorporation in Israel or its territories, with the specific intent to accomplish a boycott or divestment of Israel in a discriminatory manner. It is understood and agreed that if this certification is false, such false

certification will constitute grounds for the State to reject the bid or response submitted by the bidder or Offeror on this project and terminate any contract awarded based on the bid or response. The successful bidder or Offeror further agrees to provide immediate written notice to the contracting executive branch agency if during the term of the contract it no longer complies with this certification and agrees such noncompliance may be grounds for contract termination.

2.7. CERTIFICATION OF NO STATE LEGISLATOR INTEREST

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, Offeror hereby certifies that the Agreement is not made in violation of the South Dakota Constitution Article 3, Section 12.

2.8. MANDATORY MINIMUM REQUIREMENTS/QUALIFICATIONS

The following are mandatory minimum requirements to be evaluated on a pass/fail basis. Failure to meet any of the mandatory minimum requirements will result in rejection of the proposal.

- Commercial Off-the-Shelf (COTS) solution
- 2 projects completed in last 3 years of similar size and scope
- Software as a Service (SAAS) pricing model for seven years
- Mobile technology capability
- Ability to utilize GPS data and integrate with GIS
- Integration with State's Identity Provider to user authentication

3. PROPOSAL SUBMISSION

All proposals must be received in the Operations Support Office by the deadline in the Schedule of Activities. Proposals received after the deadline will be late and ineligible for consideration.

The proposal must be signed by an officer legally authorized to bind the Offeror to the proposal. Proposals that are not properly signed may be rejected.

The Offeror must provide an electronic copy entire proposal, including attachments, in Portable Document Format (PDF).

3.1 Electronic proposals must be submitted as an email attachment in Portable Document Format (PDF) not exceeding 15MB.

3.2 The email must be addressed to Damon.Zeltinger@state.sd.us.

3.3 Offerors should send the email using Delivery Receipt and Read Receipt options to verify successful delivery.

All materials submitted will become the property of the State of South Dakota and will be returned only at the State's option.

Offerors may modify or withdraw proposals prior to the submission deadline by contacting Damon Zeltinger at Damon.Zeltinger@state.sd.us with the subject line "RFP #24RFP9741". No oral, telephonic, telegraphic, or facsimile responses or modifications will be considered.

Offerors may email inquiries for clarification of the requirements for this RFP to Damon Zeltinger with the subject line "RFP #24RFP9741". No inquiries will be accepted after the date and time indicated in the Schedule of Activities. The Operations Support Office will respond to Offeror's inquiries via email and post all inquiries, responses, and modifications to this RFP on the State's e-procurement system. Offerors may not rely on any other statements, either of a written or oral nature, that alter any specification, term, or condition of this RFP.

Offerors and their agents (including subcontractors, employees, consultants, or anyone else acting on their behalf) must direct questions or comments regarding the RFP, the evaluation, etc. to the point of contact indicated on the first page of this RFP. Offerors and their agents may not contact any other state employee regarding these matters during the solicitation and evaluation process. Inappropriate contacts are grounds for suspension or exclusion from specific procurements.

4 PROPOSAL FORMAT

Proposals must be page numbered and include a table of contents referencing the appropriate page numbers. Maximum page limit: Twenty-five (25) 8-1/2" x 11" pages, single sided, no smaller than 11pt font. Responses to the functional and technical requirements in Appendix A, included as a separate attachment, and the South Dakota Bureau of Information and Telecommunications (BIT) Security and Vendor Questions in Appendix B, do not count against the page limit.

Proposals must be organized and tabbed with labels for the following headings:

4.1 RFP Form. The State's Proposal Submission Form must be completed and signed.

4.2 Executive Summary. The 1- or 2-page executive summary should briefly describe the major features of the Offeror's proposal. The reader should be able to determine the essence of the proposal by reading the Executive Summary. The Executive Summary must express any commitments that cannot be met by the Offeror.

Proprietary information requests must be identified in the Executive Summary. The proposal of the successful Offeror(s) will become public information. Proprietary information, such as client lists and non-public financial statements, can be protected under limited circumstances. 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 all proprietary information to be protected. The Executive Summary must specifically explain why the information is to be protected.

4.3 Relevant Experience. Provide the following information related to at least three previous or current contracts, performed by the Offeror's organization, with requirements similar to those of this RFP:

4.3.1.1 A concise description of the services performed and their requirements

4.3.1.2 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

4.3.1.3 Performance period

At a minimum, provide this information for any contract that has been terminated, expired, or not renewed in the past three years.

- 4.3.2 **Project Narrative.** A complete narrative of the Offeror's assessment of the work to be performed, the Offeror's ability and approach, and the resources necessary to fulfill the requirements, demonstrating the Offeror's understanding of the overall performance expectations.
- 4.3.3 **Technical Response.** A specific point-by-point response to the 5. Scope of Work in and the functional and technical requirements in the Microsoft Excel spreadsheet provided Appendix A of the RFP. The response should identify each requirement being addressed, as enumerated in the RFP.
- 4.3.4 **Appendix A.** A response to the functional and technical requirements to the Microsoft Excel Spreadsheet.
- 4.3.5 **Appendix B.** A response to the BIT security and vendor questions.
- 4.3.6 **Appendix C.** BIT Security Clauses
- 4.3.7 **Appendix D.** Information Technology Security Policy (ITSP) – Contractor. *NOT to be included as part of Offeror response. Provided for reference only.*
- 4.3.8 **Appendix E.** Security Acknowledgement Form. *NOT to be included as part of Offeror response. Provided for reference only.*

5 SCOPE OF WORK

5.1. INTRODUCTION

SDDOT is issuing this RFP to select a qualified Contractor to provide a COTS CMS and implementation services meeting the requirements defined in this RFP utilizing a SaaS model.

5.2. CMS FUNCTIONAL REQUIREMENTS

SDDOT desires to implement a next-generation CMS software solution (“the Solution”) and pursue the design, development, and installation of this new CMS application environment to support construction project lifecycle management.

In order to accomplish this implementation goal, SDDOT has defined system and functional requirements that the Solution will need to meet. The requirements have been categorized to align with the distinct processes of the construction project management lifecycle, specific interfaces required for the CMS, and technical framework requirements as determined by the South Dakota BIT. The functional requirements categories are:

- Contract Documents
- Manage Contract
- Measurement and Payments
- Materials Sampling and Testing
- Reports
- Finals
- Other
- Interfaces

These are described in further detail in the following sections. A complete, detailed list of functional and technical requirements is included as Appendix A Microsoft Excel Spreadsheet. Respondents are required to fill out the requirements template per the guidance in the Instructions tab.

5.2.1 Contract Documents

The primary requirement for managing contract documents for the Solution is the ability to support electronic plans, addenda and Q&A, standard and supplemental specifications, special provisions, contract forms, and executed contracts.

5.2.2 Manage Contracts

The Solution must include the ability to manage contracts throughout the project life cycle. Generally, this includes project lookup capability, summary contract information, pay items, contractor schedules, bonds, Disadvantaged Business Enterprise (DBE) requirements, and labor compliance.

5.2.3 Measurement and Payments

The Solution must provide the ability for SDDOT to manage measurement and payment processes. Generally, this includes supporting diaries, pay estimates, progress reports, visual inspections, change orders, , and checklists and job guides.

5.2.4 Materials Sampling and Testing

The Solution must provide the ability for SDDOT to manage materials sampling and testing. Generally, this includes managing standard documents (e.g., materials manuals, testing requirements, etc.), testing and certification requirements (e.g., project test requirements, testing and certification updates, etc.), certification processes (e.g., certified suppliers, materials certifications, etc.), approved products (e.g., Approved Product Lists, process documentation, validation, etc.), sampling and testing (e.g., sample data sheets, log results, mix designs, etc.), and laboratory management (e.g., log samples, progress tracking, notifications, etc.).

5.2.5 Reports

The Solution must have analytical capabilities that include a suite of standard reports and graphs to help managers at all levels manage construction projects most effectively. The Solution must allow for customizing reports, graphs, and other analysis tools to meet local or regional needs.

5.2.6 Finals

The Solution must provide SDDOT the ability to finalize projects. Generally, this includes finals review requests, project acceptance, project closeout, and include the capability to support future digital delivery and digital as-built initiatives.

5.2.7 Other/General

Electronic Project Document and File Storage and Sharing

SDDOT currently utilizes a variety of tools for project document and file storage and sharing. Examples include: Microsoft OneDrive, local network drives, File Director, Microsoft Outlook, and Microsoft SharePoint. The lack of a single source of project information has proven challenging for SDDOT. SDDOT is interested in vendors' experience and implementations of electronic document and file storage and sharing functionality to manage all internal and external communications that is intuitive and easy to use. Key aspects include a functional, easily searchable source of project information, data, and documentation. All project related agreements and permits, construction, design, etc. information should be available for easy searching and access. Outside

contractors and materials suppliers should have the ability to access and upload certain project information that is determined to be available public information. All project record retention will be in accordance with state and federal requirements.²

Formal and Region Bid Letting

SDDOT currently utilizes several in-house, custom developed tools for Formal (i.e., large scale projects) and Region Bid (i.e., smaller scale projects) Lettings (see Requirements G-12, HC10, and HC65 in the General and Interfaces Tab of the Requirements Document, Attachment A). SDDOT is interested in learning about vendors' experience and solution's capability and functionality to support Formal and Region Bid Lettings.

Disadvantaged Business Enterprise (DBE) Program Compliance³

SDDOT currently uses an in-house tool for managing DBE program compliance. SDDOT is interested in learning about Vendor offerings to support management of DBE contract requirements based on agency DBE goals and to record actual utilization and payments.

Labor Compliance

SDDOT currently uses a COTS product for monitoring and ensuring compliance with Federal labor regulations (see Requirements G-13 and 20 in the General and Interfaces Tabs, respectively, of the Microsoft Excel spreadsheet in Appendix A. SDDOT is interested in learning about Vendors' experience and solution's capability and of functionality to support all aspects of compliance with Federal and state labor regulations.

Mobile Functionality

The Solution must also provide a mobile application designed to be cross-platform. The key operating systems being considered are Apple iOS and Google Android. Also, the Solution must provide the ability to enable critical functionality of the mobile application in a connected or disconnected mode. The Solution must also provide SDDOT the ability to minimize or eliminate paper documentation. Other required functionality includes automated alerts and notifications based on SDDOT business rules and easy-to-use help functions.

5.2.8 Interfaces

The Offeror must describe how the Solution can adapt to necessary business interfaces using widely adopted open application programming interfaces (APIs) and standards. Additionally, SDDOT 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 with other business applications. A detailed description of system capability shall be included in the proposal.

The Solution must interface/integrate with the SDDOT systems documented in the Interfaces Tab of the Microsoft Excel spreadsheet included as Appendix A.

5.3. CMS NON-FUNCTIONAL REQUIREMENTS

5.3.1 User Experience

² See SDDOT Records Retention Manual for specific requirements

³ <https://dot.sd.gov/doing-business/contractors/dbe>

The Solution must provide a user experience that is simple, intuitive, and effective. It is expected that the user experience will, at minimum, allow for the ability for user configuration of commonly used screens to enable the efficient and effective processing of work tasks and intuitive solution navigation that limits the number of clicks or touches required to accomplish work tasks.

5.3.2 Solution Access and Supported Browsers

The Solution must only require internet browser software for users to access it. All State of South Dakota web sites and software will be developed using technology that is compatible with all popular, modern web browsers. No site or application will be created using proprietary features available to the visitor only when using a certain brand of web browser.

5.3.3 User Accounts and Administration

SDDOT envisions the Solution will provide a variety of user account types, from full access for system administrators to a tiered structure of limited access depending on the user's role.

It is anticipated that the Proposer will provide licensing options for modules that enable implementation of required account types. SDDOT is requesting that Proposers separate licensing into three major user groups for the purpose of providing a cost proposal:

- **Super User** – A user that is given authority within the solution to administer, manage, change, edit, configure, or create solution components able to be accessed by SDDOT and BIT personnel. Examples include stateside system administrators, Purchasing Division staff, and procurement professionals at agencies.
- **Standard User** – A user who accesses the Solution for the purpose of using tools and templates within the solution, but who does not have the ability to administer, manage, change, edit, configure, or create solution components. Examples include program staff requesting goods and services, receivers, accounts payable staff, approvers, and evaluators.
- **Non-state Employees/Contractor Access** – A non-state user who accesses the Solution for the purpose of using tools and templates within the solution, but who does not have the ability to administer, manage, change, edit, configure, or create solution components. Examples include approved contractors and administrators. The Solution shall provide the necessary security protocols to ensure the safety and security of agency data and information.

For some processes, an approval hierarchy of assigned users (or alternate approver should an approver not be available) would need to be included based on the user initializing the process and the process itself (e.g., requisition to initiate a bid for a commodity requirement: an agency or department may have several assigned personnel that approves the request before it is processed further). User accounts, based on set permissions, should have the ability to share documents (e.g., technical proposal for review) with another user and to an approved SDDOT employee that does not have a user account.

User accounts must be associated to a specific organization (e.g., agency, department, non-state entities).

Administration of the Solution, including user setup/maintenance, must have delegation assignment to allow SDDOT the option to distribute some administration responsibilities. This capability must allow definition of the specific functions and organization(s) (e.g., agencies, departments, non-state entities) that the delegated administrator will have access to manage.

5.3.4 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/> 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.

5.3.5 Office Automation Integration

SDDOT has standardized on Microsoft Office suite products (Word, Excel, PowerPoint, etc.) and Adobe. The Solution must be compatible with these products to support, at a minimum, documents as attachments, automated generation of documents (e.g., purchase orders, solicitations, contracts), import/export of transaction data (e.g., requisition line items, solicitation line items, bid tabulations, evaluation scores, contract line items), and cut/paste of text into the Solution's text fields.

5.3.6 Accessibility Requirements

Websites that are not open to the public must be secured by user login, which can be managed based on role configurations. Websites should be Americans with Disabilities Act (ADA) compliant.

5.3.7 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 Various means including but not limited to Microsoft Power BI, ESRI, Tableau and associated platforms.

5.3.8 Disaster Recovery Plan

The Contractor will have a disaster recovery plan for the Solution. This plan will document the sequence of events to follow in the circumstance that an internal or external interruption impacts services provided to the solution user community that may arise because of failure of one or more components that comprise the Solution's infrastructure,

hardware, software, interfaces, networks, Contractor's data center facility, or power. This plan will be developed in consultation with SDDOT and in adherence with the State of South Dakota Information Technology Security policies, which include Disaster Recovery standards for the State. The Contractor will provide validation reports of disaster recovery tests successes or failures on an annual basis.

The activities of the disaster recovery plan are intended to reduce or minimize downtime of critical equipment, interruption of employee work schedules, and financial exposures for SDDOT and the Contractor. This plan will also document a sequence of communication events to follow during an internal or external infrastructure failure or natural disaster (act of nature).

5.4. INTERFACE & INTEGRATION REQUIREMENTS

5.4.1 Interface Integrations

The Solution must support interface and integration capabilities in both batch and real-time. SDDOT will work with the Contractor to choose which method to employ considering costs, needs, and other factors. Proposals must provide complete technical details on these capabilities including, at a minimum, standards supported, restrictions, requirements of SDDOT systems, and whether the functionality is currently in use with existing SDDOT systems listed in the Interfaces Tab of the Microsoft Excel spreadsheet included as Appendix A.

5.4.2 Other State System Interfaces/Integrations

SDDOT anticipates that there may be other systems in use by state agencies or departments that will require either interfaces or integrations with the Solution. The development and implementation of these interfaces/integrations would be managed as a task order under the contract for the Solution, and costs for this work would be established based on the rate card established within the contract.

5.5. SOLUTION IMPLEMENTATION REQUIREMENTS

5.5.1 Implementation Approach

It is SDDOT's intent that the Solution's functionality be implemented incrementally via a phased approach based on SDDOT's priorities, which will be discussed with the selected vendor SDDOT finds high value in key functionality that includes, but is not limited to:

- Integration with existing SDDOT systems (see Interfaces Tab of the Microsoft Excel spreadsheet included as Appendix A)
- Automated routing of work based on advanced business logic
- Improved ability to intuitively view and manage workload

SDDOT prefers for functionality, once ready for implementation, to be rolled out to an initial group of pilot offices to ensure proper functionality prior to rollout to additional users. The length of the initial pilot and the future rollout schedule for functionality will be left to Proposers to detail in their implementation plan.

SDDOT intends to implement the Solution as configured to meet State process requirements, limiting any customization of the Solution to those items that must be customized to meet State statutory requirements. Where possible, SDDOT will be flexible to adopt the Solution's processes and practices to simplify implementation efforts.

SDDOT does not have a specific implementation schedule and is leaving the implementation schedule flexible to enable Proposers to provide the most effective and efficient implementation schedule for their proposed Solution, including a potential phased approach for implementation of functional requirements.

Proposers must provide details of their implementation approach in their project implementation plan. All proposal responses should be based on this implementation approach, including the project implementation plan and the cost proposal. The project implementation plan will require SDDOT approval before beginning.

5.5.2 Interface Integrations

The Contractor must plan for a project initiation phase that allows for project planning, assessment, and preparation activities prior to implementation of the Solution. This work will include, but not be limited to:

- Comprehensive review of overall project scope, contract requirements, and the responsibilities of both SDDOT, BIT and the Contractor to ensure common understanding.
- Analyze and develop specifications for all required interfaces and integrations with State systems, including any data conversion. This analysis would also identify any existing State systems that will be candidates to be retired and transitioned to the Solution. It is not the intention of the SDDOT to convert project data from the existing CMS system into the new solution.
- Develop detailed implementation strategies and recommendations for approval by SDDOT and BIT.
- Work with BIT to define an overall Solution architecture model that encompasses all interfaced and/or integrated State systems.
- Establish the initial implementation plan for the deployment and support of the Solution as architected in the previous project implementation tasks.

5.5.3 Project Staffing

The key project stakeholder roles during the CMS implementation will include the following:

- **SDDOT:** Includes all project team members from Operations, Planning and Engineering, and Finance not defined within other project roles. This category encompasses extended project team members, including application users involved in User Acceptance Testing, System Acceptance Testing, and Functional Application Reviews.
- **South Dakota Bureau of Information and Telecommunications (BIT):** Includes all project team members from this division, including management, database administrators, project coordinators, developers, and hardware and network technicians that may be required to assist with the implementation of the future CMS.

5.5.4 State Project Support

SDDOT and BIT are committed to the success of this project and will provide staffing resources as appropriate. To help SDDOT and BIT better plan to have the right resources available in the right quantities at the right time, the Proposer must provide a state

project support plan in their response. SDDOT and BIT understands that its participation is critical to ensure the goals of the project are accomplished; therefore, advanced notice of the expected SDDOT and BIT resource support required is beneficial. This should include the roles (Project Manager, architect, DBA, etc.) and amount of recommended effort during specific timeframes.

5.5.5 Training

The Proposer will be responsible for providing adequate training to ensure SDDOT's approach is met and all users identified are properly trained to utilize the implemented Solution. It is expected that the Proposer will provide personnel to develop and conduct training to the following groups at an appropriate time during implementation:

- **SDDOT End Users:** The Proposer must at a minimum provide onsite, instructor-led, computer-based, hands-on solution functionality training to key users of the initial pilot group of agencies leading up to implementation. The training will be provided in a train-the-trainer approach, being thorough enough to enable those who are trained to then train and support other SDDOT end users as needed.
- **Key Technical Resources:** The Proposer must at a minimum provide onsite, instructor-led, computer-based, hands-on training to identified technical resources sufficient to provide local technical administration of equipment and the Solution as required of SDDOT by the Proposer.
- **Help Desk and Administration:** The Proposer must at a minimum provide onsite, instructor-led, computer-based, hands-on training to identified resources sufficient to provide help desk support and perform local administration/configuration of the Solution as required of SDDOT by the Proposer.

It is expected that the Proposer will provide SDDOT with a recommended training program, including training materials and documentation sufficient for SDDOT to implement the recommended program, approach, and methods for ongoing training to include an online on-demand user experience for showing how to operate the functions of the system.

The Proposer must provide a training plan in their response that at minimum identifies the approach and method of training recommended for the various users of the Solution, both leading up to implementation of functionality and for ongoing training by SDDOT following final implementation of the Solution.

5.5.6 Testing

Testing activities will check all aspects of the Solution, including but not limited to its functionality, performance, integration, and the conversion/migration of relevant data. Since the Solution is expected to be deployed iteratively, and potentially different sets of functionalities will become available at different times, it is important to note that any additional functionality must be tested to ensure it does not negatively affect functionality already implemented or system performance.

The Contractor is responsible for all unit, Solution, performance, and regression testing of the Solution and Solution-related changes. Such changes must not be introduced into a production environment until they have been through the complete test cycle described above and approved by SDDOT after successful user acceptance testing (UAT). Test conditions and test scenarios to be included in the Solution's testing will be mutually

agreed upon by the Contractor and SDDOT. These scenarios will be based on an analysis of the requirements, changes, and modifications that are approved for implementation.

SDDOT will be responsible for UAT execution while the Contractor will be responsible for test scenario and script preparation, and management and tracking of UAT activities. UAT verifies the usability of the new processes and ensures that the Solution meets the requirements and the needs of the organization and the end user. UAT leverages Solution test scripts and is executed by SDDOT resources. The Contractor must provide all support necessary for SDDOT to successfully conduct UAT. A key objective of UAT is to facilitate an understanding of the technology and the business change being implemented.

The Contractor must also provide all support necessary for SDDOT to conduct security testing of each functional release, which may include activities such as manual testing of the Solution and loading of maliciously formatted inbound interface files.

The Contractor must remedy all bugs/defects discovered during testing in a timely manner and maintain a bug/fix tracking report that clearly identifies each bug detected in testing, the status of the resolution, and the projected fix/resolution date. The Contractor must also provide additional testing steps if needed as part of the bug fix/resolution.

The Contractor must develop and prepare weekly status reports to monitor the progress of each test phase. The status reports will contain, at a minimum, sections for condition creation, script creation, script execution, issue identification and resolution, and defect identification and resolution.

The Contractor must implement measures to avoid recurrence of incidents by performing root cause analysis and event correlation for items discovered during testing/validation activities.

5.5.7 Post-Implementation & Ongoing Support

Offerors must provide details for any and all services provided and included in their cost proposal following implementation of the Solution. Offerors should provide details of any of the following they provide and have included in their cost proposal:

- Post-implementation support to ensure the Solution is implemented and running in a stable manner without major flaws following implementation
- Help desk support
- Application support
- Solution upgrade/update support. SDDOT is interested in learning Vendor's approach for incorporating agency feedback on proposed updates, enhancements, etc. to the Vendor's Solution and associated costs, if any, to SDDOT, as well as approach for supporting SDDOT during SaaS upgrades.
- Marketplace/catalog support

6 PROPOSAL EVALUATION AND AWARD

- 6.1. Proposals may be reviewed and evaluated by any person at the discretion of the State.
- 6.2. No individual employee of the State or member of the Evaluation Committee is empowered to make binding statements regarding this RFP.
- 6.3. From the date the RFP is issued until the selection of the Contractor is announced, contact regarding this project between potential Contractors and individuals employed by the State is

restricted to written communication with the designated point of contact for this RFP. Offerors shall not attempt to communicate with or influence any evaluator involved in this RFP.

After a Contractor is selected, that Contractor is restricted from communicating with State staff other than the designated point of contact until a contract is signed. Violation of this condition may be considered sufficient cause to reject a Contractor's proposal or selection.

The following exceptions to these restrictions are permitted:

6.1.1 Contacts made pursuant to any pre-existing contracts or obligations.

6.1.2 State-requested presentations, key personnel interviews, clarification sessions, or discussions to finalize a contract.

6.4. After determining that a proposal satisfies the mandatory requirements stated in the RFP, SDDOT will evaluate all proposals utilizing a two-stage approach.

6.1.3 Stage One – Technical Response Evaluation (1,000 points)

In stage one, the State's evaluator(s) will use subjective judgment to conduct a comparative assessment of the proposal by considering the following criteria:

EVALUATION CRITERIA	Points Possible
1. Project Organizational Structure/Key Personnel (50 points)	
Experience and credentials of key personnel project team	25
Recent experience of team working together	25
2. Projects/Experience Record of Past Performance, including Price and Cost Data from Previous Projects, Quality of Work, Ability to Meet Schedules, Cost Control, and Contract Administration (125 points)	
Successful and recent similarly scoped project experience	50
Demonstrated past capability to deliver scope on time and within budget	50
Reference letters	25
3. Firm's Implementation Capability and Resources Available to Perform the Work, including Any Specialized Services, within the Specified Time Limits for the Project (300 points)	
Implementation approach	150
Project and change management approach	75
QA/QC and testing plan	75
4. Solution's Capability and Suitability (500 points)	
Ability to meet mandatory requirements out of the box or with configuration	300
Ability to interact/interface with SDDOT key systems and user experience	100
Ability to deliver promised SaaS uptime	25
Querying and reporting capabilities	75
1. Contractor's Availability to and Familiarity with Project Locale (20 points)	
Contractor's familiarity with South Dakota or with Agencies that have a similar scope and environment	10
Contractor's ability to have staff on site if needed as well as virtually	10
2. Contractor's Ability and Proven History in Handling Special Project Constraints (5 points)	
The Vendor should provide examples of how they have dealt with unanticipated circumstances	5

6.1.4 Stage Two – Vendor Demonstration and Cost Proposals (1,000 Points)

Following the review by the State's evaluators, the Offeror's proposed solutions will be ranked. SDDOT intends to select up to three vendors to participate in scripted demonstrations of the proposed solutions. These in-person demonstrations will follow the functional and technical requirements for the Solution as shown in the Microsoft Excel Spreadsheet in Appendix A and provide the Offeror the opportunity meet with the SDDOT project team and evaluators. SDDOT expects that log-ins for each proposed solution will be provided for up to twenty-five SDDOT personnel. This provides SDDOT personnel an opportunity to work with the proposed solution in a test or "sandbox" environment. Proposed dates for the short-listed vendor demonstrations are shown in the schedule of activities in Section 1.3 and it is expected that Offerors will be available. Offerors will be

randomly assigned a presentation date. It is required that the Offeror's proposed project manager and implementation lead will be present at the demonstration. Scores from Stage One will not impact the scoring for Stage Two.

6.1.4.1 Short-Listed Vendor Demonstration (800 points)

SDDOT intends to conduct up to three scripted vendor demonstrations of the Offeror's proposed solutions. SDDOT reserves the right to revise the agenda for the demonstrations, but a preliminary approach is as follows.

Offeror should plan to demonstrate specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements.

SDDOT data will be provided to the Offeror ahead of the demonstration and must be used by the Offeror. These demonstrations are expected to be two days in length and include demonstrations of both desktop and mobile functionality. The Offeror will be provided with an opportunity to deliver a closing presentation at the completion of day 2.

6.1.4.2 Cost Proposals (200 points)

Cost proposals are not to be submitted at the time the technical proposals are due. Cost proposals are only due from Offerors that are invited to the vendor demonstration. Cost proposals should be sent to the Procurement Officers by the date defined in the schedule of activities in Section 1.3.

Cost proposals will be evaluated in conjunction with vendor demonstrations. The total amount of points allocated to stage 2 is 1,000 points, with vendor demonstrations representing 800 possible points, and cost proposals representing 200 possible points. Offerors shall be sent the vendor demonstration evaluation criteria if invited to stage 2.

The points assigned to each Offeror's cost proposal will be based on the lowest proposal price. The Offeror with the lowest proposed price will receive 100% of the price points. All other Offerors will receive a portion of the total cost points based on what percentage higher their proposed price is than the lowest proposed price. An Offeror whose proposed price is more than double (200%) the lowest proposed price will receive no points.

When pricing information is provided, it should delineate the complete upfront and ongoing costs. Items such as, but not limited to, development costs, license costs, new report/query creation costs, consulting costs, support costs, on-call costs, access costs, hosting costs, third-party costs, etc. must be included.

- 6.5. 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.
- 6.6. 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.

- 6.7. The State reserves the right to review all aspects of the cost proposal for reasonableness and to request clarification of any proposal where the cost component shows significant and unsupported deviation from industry standards or in areas where detailed pricing is required.
- 6.8. This procurement is a Request for Proposal/Competitive Negotiation process. Each proposal will be evaluated, and each respondent will be available for negotiation meetings at the State's request. The State reserves the right to negotiate on any elements 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 will be kept confidential. The negotiation discussions will also be held as confidential until the award is completed.
- 6.8.1 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.
- 6.8.2 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.
- 6.8.3 The negotiation process may continue through successive Offerors, according to agency ranking, until an agreement is reached, or the agency terminates the contracting process.

7 STANDARD CONTRACT TERMS AND CONDITIONS

- 7.1. Any contract or agreement resulting from this RFP will include the State's standard I/T contract terms listed in Appendix C, along with any additional contract terms as negotiated by the parties. As part of the negotiation process the contract terms listed here in Section 7 and Appendix C 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.
- 7.2. The Contractor will perform those services described in the Contractor's proposal, attached hereto and by this reference incorporated herein.
- 7.3. Contractor's services under this Agreement shall begin on Day 1 following execution of the contract for a period of seven years.
- 7.4. 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.

- 7.5. The State will make payment for services upon satisfactory completion of the services. The TOTAL CONTRACT AMOUNT is an amount not to exceed (to be determined). 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 ch. 5-26.
- 7.6. The Contractor agrees to indemnify and hold the State of South Dakota, its officers, agents, and employees, harmless from and against any and all actions, suits, damages, liability, or other proceedings that may arise as the result of performing services hereunder. This section does not require the Contractor to be responsible for or defend against claims or damages arising solely from errors or omissions of the State, its officers, agents, or employees.
- 7.7. Throughout the term of this Agreement, the Contractor shall obtain and maintain in force insurance coverage of the following types and limits:
- 7.7.1 Commercial General Liability Insurance: The Contractor shall maintain occurrence based commercial general liability insurance or equivalent form with a limit of not less than \$1,000,000 for each occurrence. If such insurance contains a general aggregate limit it shall apply separately to this Agreement or be no less than two times the occurrence limit.
- 7.7.2 Professional Liability Insurance or Miscellaneous Professional Liability Insurance: The Contractor agrees to procure and maintain professional liability insurance or miscellaneous professional liability insurance with a limit not less than \$1,000,000.
- 7.7.3 Business Automobile Liability Insurance: The Contractor shall maintain business automobile liability insurance or equivalent form with a limit not less than \$1,000,000 for each accident. Such insurance shall include coverage for owned, hired, and non-owned vehicles.
- 7.7.4 Worker's Compensation Insurance: The Contractor shall 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 clearly evidencing all insurance required in this Agreement. In the event a substantial change in insurance, issuance of a new policy, or 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.
- 7.8. While performing services hereunder, the Contractor is an independent contractor and not an officer, agent, or employee of the State of South Dakota.
- 7.9. Contractor agrees to report to the State any event encountered during the performance of this Agreement that results in injury to the person or property of third parties or which may otherwise subject Contractor or the State to liability. Contractor will report any such event to the State immediately upon discovery.
- 7.10. 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 required by their duties or applicable law. Contractor's obligation to report will not require disclosure of any information subject to privilege or confidentiality under law. Reporting to the State under this

section will not excuse or satisfy any obligation of Contractor to report any event to law enforcement or other entities under the requirements of any applicable law.

- 7.11. This Agreement may be terminated by either party hereto upon thirty (30) days written notice. In the event the Contractor breaches any of the terms or conditions hereof, this Agreement may be terminated by the State at any time with or without notice. If termination for such a default is effected by the State, any payments due to Contractor at the time of termination may be adjusted to offset additional costs to the State because of Contractor's default. Upon termination the State may assume the work and award another party an agreement to complete the work. If, after the State terminates for a default by Contractor, it is determined that Contractor was not at fault, the Contractor will be paid for eligible services rendered and expenses incurred up to the date of termination.
- 7.12. 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.
- 7.13. This Agreement may not be assigned without the express prior written consent of the State. This Agreement may not be amended except in writing expressly identified as a part hereof and signed by an authorized representative of each of the parties hereto.
- 7.14. 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.
- 7.15. 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.
- 7.16. The Contractor may not use subcontractors to perform the services described herein without the express 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.
- 7.17. Contractor hereby acknowledges and agrees that all reports, plans, specifications, technical data, miscellaneous drawings, software system programs and documentation, procedures, or files, operating instructions and procedures, source code(s) and documentation, including those necessary to upgrade and maintain the software program, and all information contained therein provided to the State by the Contractor in connection with its performance of services under this Agreement shall belong to and is the property of the State and will not be used in any way by the Contractor without the written consent of the State. Papers, reports, forms, software programs, source code(s) and other material which are a part of the work under this Agreement will not be copyrighted without written approval of the State.

- 7.18. 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.
- 7.19. 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 (to be named) on behalf of the State, and by (to be named), 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.
- 7.20. If any court of competent jurisdiction holds any provision of this Agreement unenforceable or invalid, such holding will not invalidate or render unenforceable any other provision hereof.
- 7.21. All other prior discussions, communications and representations concerning the subject matter of this Agreement are superseded by the terms of this Agreement, and except as specifically provided herein, this Agreement constitutes the entire agreement with respect to the subject matter hereof.

8 PROJECT DELIVERABLES/APPROACH/METHODOLOGY

- 8.1. The Offeror must 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.
- 8.2. 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.
- 8.3. 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.
- 8.4. 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.

- 8.5. 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.
- 8.6. 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.
- 8.7. 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)
- 8.8. 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.
- 8.9. 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.

8.10. 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.

8.11. 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.

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

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

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

8.13.1 Include in your submission details on your:

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

8.14. 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.

8.15. The offeror’s solution cannot include any hardware or hardware components manufactured by Huawei Technologies Company or ZTE Corporation or any subsidiary or affiliate of such entities. This includes hardware going on the State’s network as well as the 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.

- 8.16. 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.

9 NON-STANDARD HARDWARE AND SOFTWARE

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

10 BACKGROUND CHECKS

- 10.1. 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.

Appendix A

A specific point-by-point response to the scope of work in Section 5 and the functional and technical requirements provided in the Microsoft Excel spreadsheet (separate attachment in the RFP documentation). The response should identify each requirement being addressed, as enumerated in the RFP and the Proposer shall return the completed Microsoft Excel spreadsheet as part of proposal submission.

Appendix B

Security and Vendor Questions

Basic Vendor Information

Vendor Legal Name:

Vendor Address:

Directions

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

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

Vendors: The following questions help the State determine the best way to assess and integrate your product or service technology with the State's technology infrastructure. 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 that a Yes/No/NA response is not appropriate, the cell has been grayed out. **If the vendor answers a question by referencing another document or another part of the RFP response, the vendor must provide the page number and paragraph where the information can be found.**

The "BIT" column corresponds to the division within BIT that will be the primary reviewers. If you have questions about the meaning or intent of a question, we can contact the BIT division on your behalf. DC = Data Center; DEV = Development; TEL = Telecommunications; POC = Point of 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)
4	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)
5	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
6	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:
7	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:
8	POC	If there are desktop software installs, please provide a link to the licensing requirements or a copy of the licensing requirements.	Please provide link below, if applicable:
9	POC	Will any hardware or peripherals need to be attached to or added to state managed computers?	<input type="checkbox"/> Yes <input type="checkbox"/> No If "Yes", please define:
10	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:
11	POC	Will any products that connect or interact with a state managed computer or network be required as part of this product or project?	<input type="checkbox"/> Yes <input type="checkbox"/> No If "Yes", please define:
12	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:
13	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
14	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 upmost importance. Web Application Vulnerability Scans must be done if:</p> <ul style="list-style-type: none"> • An application will be placed on the State's system. • The State's system connects to another system. • The contractor hosts State data. • The contractor has another party host State data the State will want to scan that party. <p><u>The State would want to scan a test system; not a production system and will not do penetration testing.</u> 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)?				
A10	DEV	Are there any additional components or configurations required outside of the base product to meet the State's security needs?				
A11	TEL	What threat assumptions were made, if any, when designing protections for the software and information assets processed?				
A12	TEL	How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used?				
A13	TEL	What security criteria, if any, are considered when selecting third party suppliers?				
A14	TEL	How has the software been measured/assessed for its resistance to publicly known vulnerabilities and/or attack patterns identified in the Common Vulnerabilities & Exposures (CVE®) or Common Weakness Enumerations (CWEs)? How have the findings been mitigated?				
A15	TEL	Has the software been evaluated against the Common Criteria, FIPS 140-3, 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.				
A16	DC TEL	Are static or dynamic software security analysis tools used to identify weaknesses in the software that can lead to exploitable vulnerabilities? If yes, which tools are used? What classes of weaknesses are covered? When in the SDLC are these scans performed? Are SwA experts involved in the analysis of the scan results?				
A17	DC TEL x	Has the product undergone any vulnerability or penetration testing? If yes, how frequently, by whom, and are the test reports available under a nondisclosure agreement? How have the findings been mitigated?				
A18	DC	Does your company have an executive-level officer responsible for the security of your company's software products and/or processes?				
A19	DC	How are software security requirements developed?				
A20	DC	What risk management measures are used during the software's design to mitigate risks posed by use of third-party components?				

A21	DC	What is your background check policy and procedure? Are your background checks fingerprint based? If required, would you be willing to undergo fingerprint-based background checks?				
A22	DEV	Does your company have formally defined security policies associated with clearly defined roles and responsibilities for personnel working within the software development life cycle? Explain.				
A23	TEL	What are the policies and procedures used to protect sensitive information from unauthorized access? How are the policies enforced?				
A24	DC TEL	Do you have an automated Security Information and Event Management system?				
A25	DC TEL	What types of event logs do you keep and how long do you keep them?				
		a. System events				
		b. Application events				
		c. Authentication events				
		d. Physical access to your data center(s)				
		e. Code changes				
		f. Other:				
A26	DC	How are security logs and audit trails protected from tampering or modification? Are log files consolidated to single servers?				
A27	DEV	a. Are security specific regression tests performed during the development process?				
		b. If yes, how frequently are the tests performed?				
A28	TEL	What type of firewalls (or application gateways) do you use? How are they monitored/managed?				
A29	TEL	What type of Intrusion Detection System/Intrusion Protection Systems (IDS/IPS) do you use? How are they monitored/managed?				
A30	DC TEL	What are your procedures for intrusion detection, incident response, and incident investigation and escalation?				
A31	DC TEL	Do you have a BYOD policy that allows your staff to put any sort of sensitive or legally protected State data on their device personal device(s) or other non-company owned system(s)?				

A32	DC TEL	Do you require multifactor authentication be used by employees and subcontractors who have potential access to legally protected State data or administrative control? If yes, please explain your practices on multifactor authentication including the authentication level used as defined in NIST 800-63 in your explanation. If no, do you plan on implementing multifactor authentication? If so, when?				
A33	POC	Will this system provide the capability to track data entry/access by the person, date, and time?				
A34	DC DEV POC TEL	Will the system provide data encryption for sensitive or legally protected information both at rest and transmission? If yes, please provide details.				
A35	DC	a. Do you have a SOC 2 or ISO 27001 audit report?				
		b. Is the audit performed annually?				
		c. 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.				
A36	DC	Do you or your cloud service provider have any other security certification beside SOC 2 or ISO 27001, for example, FedRAMP or HITRUST?				
A37	DC TEL	Are you providing a device or software that can be defined as being Internet of Thing (IoT)? Examples include IP camera, network printer, or connected medical device. If yes, what is your process for ensuring the software on your IoT devices that are connected to the state's system, either permanently or intermittently, are maintained and/or updated?				

A38	DC	Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all registry settings?				
A39	DC	What are your policies and procedures for hardening servers?				
A40	DC TEL	(Only to be used when medical devices are being acquired.) Please give the history of cybersecurity advisories issued by you for your medical devices. Include the device, date, and the nature of the cybersecurity advisory.				
A41	DC POC	Does any product you propose to use or provide the State include software, hardware, or hardware components manufactured by any company on the federal government's Entity List?				
A42	DC	Describe your process for monitoring the security of your suppliers.				

Section B. Hosting

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

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

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

Response

#	BIT	Question	YES	NO	NA	Explain answer as needed
B1	POC	Are there expected periods of time where the application will be unavailable for use?				
B2	DC	If you have agents or scripts executing on servers of hosted applications what are the procedures for reviewing the security of these scripts or agents?				
B3	DC	What are the procedures and policies used to control access to your servers? How are audit logs maintained?				
B4	DC DEV POC TEL	Do you have a formal disaster recovery plan? Please explain what actions will be taken to recover from a disaster. Are warm or hot backups available? What are the Recovery Time Objectives and Recovery Point Objectives?				
B5	DC	Explain your tenant architecture and how tenant data is kept separately?				
B6	DC	What are your data backup policies and procedures? How frequently are your backup procedures verified?				
B7	DC DEV TEL	If any cloud services are provided by a third-party, do you have contractual requirements with them dealing with: <ul style="list-style-type: none">• Security for their I/T systems;• Staff vetting;• Staff security training?				
		a. If yes, summarize the contractual requirements.				
		b. If yes, how do you evaluate the third-party's adherence to the contractual requirements?				
B8	DC	If your application is hosted by you or a third party, are all costs for your software licenses in addition to third-party software (i.e. MS-SQL, MS Office, and Oracle) included in your cost proposal? If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized?				
B9	DC	a. Do you use a security checklist when standing up any outward facing system?				

		b. Do you test after the system was stood up to make sure everything in the checklist was correctly set?				
B10	DC	How do you secure Internet of Things (IoT) devices on your network?				
B11	DC TEL	Do you use Content Threat Removal to extract and transform data?				
B12	DC TEL	Does your company have an endpoint detection and response policy?				
B13	DC TEL	Does your company have any real-time security auditing processes?				
B14	TEL	How do you perform analysis against the network traffic being transmitted or received by your application, systems, or data center? What benchmarks do you maintain and monitor your systems against for network usage and performance? What process(es) or product(s) do you use to complete this analysis, and what results or process(es) can you share?				
B15	TEL	How do you monitor your application, systems, and data center for security events, incidents, or information? What process(es) and/or product(s) do you use to complete this analysis, and what results or process(es) can you share?				
B16	DC TEL	What anti-malware product(s) do you use?				
B17	DC TEL	What is your process to implement new vendor patches as they are released and what is the average time it takes to deploy a patch?				
B18	DC TEL	Have you ever had a data breach? If so, provide information on the breach.				
B19	POC	Is there a strategy for mitigating unplanned disruptions and what is it?				
B20	DC TEL	What is your process for ensuring the software on your IoT devices that are connected to your system, either permanently or intermittently, is maintained and updated?				
B21	POC	Will the State of South Dakota own the data created in your hosting environment?				
B22	DEV	What are your record destruction scheduling capabilities?				

Section C: Database

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

Response

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

Section D: Contractor Process

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

Response

#	BIT	Question	YES	NO	NA	Explain answer as needed
D1	DC POC	Will the vendor provide assistance with installation?				
D2	DC DEV POC TEL	Does your company have a policy and process for supporting/requiring professional certifications? If so, how do you ensure certifications are valid and up-to date?				
D3	DEV	What types of functional tests are/were performed on the software during its development (e.g., spot checking, component-level testing, and integrated testing)?				
D4	DEV	Are misuse test cases included to exercise potential abuse scenarios of the software?				
D5	TEL	What release criteria does your company have for its products regarding security?				
D6	DEV	What controls are in place to ensure that only the accepted/released software is placed on media for distribution?				
D7	DC DEV	a. Is there a Support Lifecycle Policy within the organization for the software				
		b. Does it outline and establish a consistent and predictable support timeline?				
D8	DC	How are patches, updates, and service packs communicated and distributed to the State?				
D9	DEV	What services does the help desk, support center, or (if applicable) online support system offer when are these services available, and are there any additional costs associated with the options?				
D10	DC	a. Can patches and service packs be uninstalled?				
		b. Are the procedures for uninstalling a patch or service pack automated or manual?				
D11	DC DEV	How are enhancement requests and reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, prioritized, and reported? Is the management and reporting policy available for review?				
D12	DC	What are your policies and practices for reviewing design and architecture security impacts in relation to deploying patches, updates, and service packs?				
D13	DC	Are third-party developers contractually required to follow your configuration management and security policies and how do you assess their compliance?				
D14	DEV	What policies and processes does your company use to verify that your product has its comments sanitized and does not contain undocumented				

		functions, test/debug code, or unintended, “dead,” or malicious code? What tools are used?				
D15	DEV	How is the software provenance verified (e.g., any checksums or signatures)?				
D16	DEV	a. Does the documentation explain how to install, configure, and/or use the software securely?				
		b. Does it identify options that should not normally be used because they create security weaknesses?				
D17	DEV	a. Does your company develop security measurement objectives for all phases of the SDLC?				
		b. Has your company identified specific statistical and/or qualitative analytical techniques for measuring attainment of security measures?				
D18	DC	a. Is testing done after changes are made to servers?				
		b. What are your rollback procedures in the event of problems resulting from installing a patch or service pack?				
D19	DC	What are your procedures and policies for handling and destroying sensitive data on electronic and printed media?				
D20	DC TEL	How is endpoint protection done? For example, is virus prevention used and how are detection, correction, and updates handled?				
D21	DC TEL	Do you perform regular reviews of system and network logs for security issues?				
D22	DC	Do you provide security performance measures to the customer at regular intervals?				
D23	DC POC	What technical, installation, and user documentation do you provide to the State? Is the documentation electronically available and can it be printed?				
D24	DC DEV POC	a. Will the implementation plan include user acceptance testing?				
		b. If yes, what were the test cases?				
		c. Do you do software assurance?				
D25	DC DEV POC TEL	Will the implementation plan include performance testing?				
D26	DEV POC	Will there be documented test cases for future releases including any customizations done for the State of South Dakota?				
D27	DEV POC	If the State of South Dakota will gain ownership of the software, does the proposal include a knowledge transfer plan?				
D28	DEV POC	Has your company ever conducted a project where your product was load tested?				

D29	DC	Please explain the pedigree of the software. Include in your answer who are the people, organization, and processes that created the software.				
D30	DC	Explain the change management procedure used to identify the type and extent of changes allowed in the software throughout its lifecycle. Include information on the oversight controls for the change management procedure.				
D31	DC DEV TEL	Does your company have corporate policies and management controls in place to ensure that only corporate-approved (licensed and vetted) software components are used during the development process? Provide a brief explanation. Will the supplier indemnify the acquirer from these issues in the license agreement? Provide a brief explanation.				
D32	DEV	Summarize the processes (e.g., ISO 9000, CMMi), methods, tools (e.g., IDEs, compilers), techniques, etc. used to produce and transform the software.				
D33	DEV	a. Does the software contain third-party developed components?				
		b. If yes, are those components scanned by a static code analysis tool?				
D34	DC DEV TEL	What security design and security architecture documents are prepared as part of the SDLC process? How are they maintained? Are they available to/for review?				
D35	DEV	Does your organization incorporate security risk management activities as part of your software development methodology? If yes, please provide a copy of this methodology or provide information on how to obtain it from a publicly accessible source.				
D36	DC	Does your company ever perform site inspections/policy compliance audits of its U.S. development facilities? Of its non-U.S. facilities? Of the facilities of its third-party developers? If yes, how often do these inspections/audits occur? Are they periodic or triggered by events (or both)? If triggered by events, provide examples of "trigger" events.				
D37	DC TEL	How are trouble tickets submitted? How are support issues, specifically those that are security-related escalated?				
D38	DC DEV	Please describe the scope and give an overview of the content of the security training you require of your staff, include how often the training is given and to whom. Include training specifically given to your developers on secure development.				
D39	DC TEL x	It is State policy that all Contractor Remote Access to systems for support and maintenance on the State Network will only be allowed through Citrix Netscaler. Would this affect the implementation of the system?				

D40	POC TEL x	Contractors are also expected to reply to follow-up questions in response to the answers they provided to the security questions. At the State's discretion, a contractor's answers to the follow-up questions may be required in writing and/or verbally. The answers provided may be used as part of the contractor selection criteria. Is this acceptable?				
D41	DC DEV POC TEL x	(For PHI only) a. Have you done a risk assessment? If yes, will you share it?				
		b. If you have not done a risk assessment, when are you planning on doing one?				
		c. If you have not done a risk assessment, would you be willing to do one for this project?				
D42	DEV POC	Will your website conform to the requirements of Section 508 of the Rehabilitation Act of 1973?				

Section E: Software Development

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

Response

#	BIT	Question	YES	NO	NA	Explain answer as needed.
E1	DEV POC x	What are the development technologies used for this system?				If marked yes, indicate version.
		ASP.Net				
		VB.Net				
		C#.Net				
		.NET Framework				
		Java/JSP				
		MS SQL				
		Other				
E2	DC TEL	Is this a browser-based user interface?				
E3	DEV POC	Will the system have any workflow requirements?				
E4	DC	Can the system be implemented via Citrix?				
E5	DC	Will the system print to a Citrix compatible networked printer?				
E6	TEL	If your application does not run under the latest Microsoft operating system, what is your process for updating the application?				
E7	DEV	Identify each of the Data, Business, and Presentation layer technologies your product would use and provide a roadmap outlining how your release or update roadmap aligns with the release or update roadmap for this technology.				
E8	TEL x	Will your system use Adobe Air, Adobe Flash, Adobe ColdFusion, Apache Flex, Microsoft Silverlight, PHP, Perl, Magento, or QuickTime? If yes, explain?				
E9	DEV	To connect to other applications or data, will the State be required to develop custom interfaces?				
E10	DEV	To fulfill the scope of work, will the State be required to develop reports or data extractions from the database? Will you provide any APIs that the State can use?				
E11	DEV POC	Has your company ever integrated this product with an enterprise service bus to exchange data between diverse computing platforms?				
E12	DC	a. If the product is hosted at the State, will there be any third-party application(s) or system(s) installed or embedded to support the product (for example, database software, run libraries)?				
		b. If yes, please list those third-party application(s) or system(s).				
E13	DEV	What coding and/or API standards are used during development of the software?				

E14	DEV	Does the software use closed-source Application Programming Interfaces (APIs) that have undocumented functions?				
E15	DEV	How does the software's exception handling mechanism prevent faults from leaving the software, its resources, and its data (in memory and on disk) in a vulnerable state?				
E16	DEV	Does the exception handling mechanism provide more than one option for responding to a fault? If so, can the exception handling options be configured by the administrator or overridden?				
E17	DEV	What percentage of code coverage does your testing provide?				
E18	DC	a. Will the system infrastructure involve the use of email?				
		b. Will the system infrastructure require an interface into the State's email infrastructure?				
		c. Will the system involve the use of bulk email distribution to State users? Client users? In what quantity will emails be sent, and how frequently?				
E19	TEL x	a. Does your application use any Oracle products?				
		b. If yes, what product(s) and version(s)?				
		c. Do you have support agreements for these products?				
E20	DC	Explain how and where the software validates (e.g., filter with whitelisting) inputs from untrusted sources before being used.				
E21	TEL	a. Has the software been designed to execute within a constrained execution environment (e.g., virtual machine, sandbox, chroot jail, single-purpose pseudo-user)?				
		b. Is it designed to isolate and minimize the extent of damage possible by a successful attack?				
E22	TEL	Does the program use run-time infrastructure defenses (such as address space randomization, stack overflow protection, preventing execution from data memory, and taint checking)?				
E23	TEL	If your application will be running on a mobile device, what is your process for making sure your application can run on the newest version of the mobile device's operating system?				
E24	DEV	Do you use open-source software or libraries? If yes, do you check for vulnerabilities in your software or library that are listed in:				
		a. Common Vulnerabilities and Exposures (CVE) database?				
		b. Open Web Application Security Project (OWASP) Top Ten?				

F. Infrastructure

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

Response

#	BIT	Question	YES	NO	NA	Explain answer as needed.
F1	DC	Will the system infrastructure have a special backup requirement?				
F2	DC	Will the system infrastructure have any processes that require scheduling?				
F3	DC	The State expects to be able to move your product without cost for Disaster Recovery purposes and to maintain high availability. Will this be an issue?				
F4	TEL x	Will the network communications meet Institute of Electrical and Electronics Engineers (IEEE) standard TCP/IP (IPv4, IPv6) and use either standard ports or State-defined ports as the State determines?				
F5	DC x	It is State policy that all systems must be compatible with BIT's dynamic IP addressing solution (DHCP). Would this affect the implementation of the system?				
F6	TEL x	It is State policy that all software must be able to use either standard Internet Protocol ports or Ports as defined by the State of South Dakota BIT Network Technologies. Would this affect the implementation of the system? If yes, explain.				
F7	DC	It is State policy that all HTTP/SSL communication must be able to be run behind State of South Dakota content switches and SSL accelerators for load balancing and off-loading of SSL encryption. The State encryption is also PCI compliant. Would this affect the implementation of your system? If yes, explain.				
F8	DC x	The State has a virtualize first policy that requires all new systems to be configured as virtual machines. Would this affect the implementation of the system? If yes, explain.				
F9	TEL x	It is State policy that all access from outside of the State of South Dakota's private network will be limited to set ports as defined by the State and all traffic leaving or entering the State network will be monitored. Would this affect the implementation of the system? If yes, explain.				
F10	TEL	It is State policy that systems must support Network Address Translation (NAT) and Port Address Translation (PAT) running inside the State Network. Would this affect the implementation of the system? If yes, explain.				
F11	TEL x	It is State policy that systems must not use dynamic Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports unless the system is a well-known one that is state firewall supported (FTP, TELNET, HTTP, SSH, etc.). Would				

		this affect the implementation of the system? If yes, explain.				
F12	DC	The State of South Dakota currently schedules routine maintenance from 0400 to 0700 on Tuesday mornings for our non-mainframe environments and once a month from 0500 to 1200 for our mainframe environment. Systems will be offline during this scheduled maintenance time periods. Will this have a detrimental effect to the system?				
F13	POC TEL	Please describe the types and levels of network access your system/application will require. This should include, but not be limited to TCP/UDP ports used, protocols used, source and destination networks, traffic flow directions, who initiates traffic flow, whether connections are encrypted or not, and types of encryption used. The Contractor should specify what access requirements are for user access to the system and what requirements are for any system level processes. The Contractor should describe all requirements in detail and provide full documentation as to the necessity of the requested access.				
F14	POC x	List any hardware or software you propose to use that is not State standard, the standards can be found at: https://bit.sd.gov/bit?id=bit_standards_overview .				
F15	DC	Will your application require a dedicated environment?				
F16	DEV POC	Will the system provide an archival solution? If not, is the State expected to develop a customized archival solution?				
F17	DC TEL	Provide a system diagram to include the components of the system, description of the component, and how the components communicate with each other.				
F18	DC	Can the system be integrated with our enterprise Active Directory to ensure access is controlled?				
F19	TEL x	It is State policy that no equipment can be connected to State Network without direct approval of BIT Network Technologies. Would this affect the implementation of the system?				
F20	DC x	Will the server-based software support:				
		a. Windows server 2016 or higher				
		b. IIS7.5 or higher				
		c. MS SQL Server 2016 standard edition or higher				
		d. Exchange 2016 or higher				
		e. Citrix XenApp 7.15 or higher				
		f. VMWare ESXi 6.5 or higher				
		g. MS Windows Updates				
		h. Windows Defender				

F21	TEL x	All network systems must operate within the current configurations of the State of South Dakota's firewalls, switches, IDS/IPS, and desktop security infrastructure. Would this affect the implementation of the system?				
F22	DC	All systems that require an email interface must use SMTP Authentication processes managed by BIT Datacenter. Mail Marshal is the existing product used for SMTP relay. Would this affect the implementation of the system?				
F23	DC TEL	The State implements enterprise-wide anti-virus solutions on all servers and workstations as well as controls the roll outs of any and all Microsoft patches based on level of criticality. Do you have any concerns regarding this process?				
F24	DC TEL	What physical access do you require to work on hardware?				
F25	DC	How many of the vendor's staff and/or subcontractors will need access to the state system, will this be remote access, and what level of access will they require?				

Section G: Business Process

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

Response

#	BIT	Question	YES	NO	NA	Explain answer as needed.
G1	DC	a. If your application is hosted on a dedicated environment within the State's infrastructure, are all costs for your software licenses in addition to third-party software (i.e. MS-SQL, MS Office, and Oracle) included in your cost proposal?				
		b. If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized?				
G2	POC	Explain the software licensing model.				
G3	DC DEV POC	Is on-site assistance available? If so, what is the charge?				
G4	DEV POC	a. Will you provide customization of the system if required by the State of South Dakota?				
		b. If yes, are there any additional costs for the customization?				
G5	POC	Explain the basis on which pricing could change for the State based on your licensing model.				
G6	POC	Contractually, how many years price lock will you offer the State as part of your response? Also, as part of your response, how many additional years are you offering to limit price increases and by what percent?				
G7	POC	Will the State acquire the data at contract conclusion?				
G8	POC	Will the State's data be used for any other purposes other than South Dakota's usage?				
G9	DC	Has your company ever filed for Bankruptcy under U.S. Code Chapter 11? If so, please provide dates for each filing and describe the outcome.				
G10	DC	Has civil legal action ever been filed against your company for delivering or failing to correct defective software? Explain.				
G11	DC	Please summarize your company's history of ownership, acquisitions, and mergers (both those performed by your company and those to which your company was subjected).				
G12	DC	Will you provide on-site support 24x7 to resolve security incidents? If not, what are your responsibilities in a security incident?				
G13	DEV	What training programs, if any, are available or provided through the supplier for the software? Do you offer certification programs for software integrators? Do you offer training materials, books, computer-based training, online educational				

		forums, or sponsor conferences related to the software?				
G14	DC TEL	Are help desk or support center personnel internal company resources or are these services outsourced to third parties? Where are these resources located?				
G15	DC	Are any of the professional services you plan to provide located outside the United States (e.g., help desk or transcription services)?				
G16	DC	Is the controlling share (51%+) of your company owned by one or more non-U.S. entities?				
G17	DC	What are your customer confidentiality policies? How are they enforced?				
G18	DC POC 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?				
G19	DC	If the product is hosted at the State, will there be a request to include an application to monitor license compliance?				
G20	DC POC	Is telephone assistance available for both installation and use? If yes, are there any additional charges?				
G21	DC TEL	What do you see as the most important security threats your industry faces?				

Appendix C BIT Clauses

Bureau of Information and Telecommunications

Required IT Contract Terms

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

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

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

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

Section I. Confidentiality of Information

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

agreed in a writing signed by both parties. State Proprietary Information will not include information that:

- (i) was in the public domain at the time it was disclosed to the Vendor,
- (ii) was known to the Vendor without restriction at the time of disclosure from the State,
- (iii) that was disclosed with the prior written approval of State's officers or employees having authority to disclose such information,
- (iv) was independently developed by the Vendor without the benefit or influence of the State's information, and
- (v) 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. 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 V. 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 VI. 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 VII. 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 VIII. 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 IX. 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 X. 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 XI. Audit Requirements

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

Section XII. Annual Risk Assessment

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

- A. Penetration testing of the Vendor's system;
- B. Security policies and procedures;

- C. Disaster recovery plan;
- D. Business Associate Agreements; and
- E. Inventory of physical systems, devices, and media that store or utilize ePHI for completeness.

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

Section XIII. Independent Audit

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

Section XIV. 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 XV. 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 XVI. 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:

- i) Contract dispute between the parties to this Agreement,
- ii) There is a billing dispute between the parties to this Agreement, or
- iii) The Vendor merges with or is acquired by another company.

Section XVII. 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 XVIII. 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 XIX. 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 XX. Security Incident Notification for Non-Health Information

The Vendor will implement, maintain, and update Security Incident procedures that comply with all State standards and Federal and State requirements. A Security Incident is a violation of any BIT security or privacy policies or contract agreements involving sensitive information, or the imminent threat of a violation. The BIT security policies can be found in the Information Technology Security Policy ("ITSP") attached as BIT Attachment 1. The State requires notification of a Security Incident involving any of the State's sensitive data in the Vendor's possession. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party. The parties agree that, to the extent probes and reconnaissance scans

common to the industry constitute Security Incidents, this Agreement constitutes notice by the Vendor of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State will be required. Probes and scans include, without limitation, pings and other broadcast attacks in the Vendor's firewall, port scans, and unsuccessful log-on attempts, if such probes and reconnaissance scans do not result in a Security Incident as defined above. Except as required by other legal requirements the Vendor will only provide notice of the incident to the State. The State will determine if notification to the public will be by the State or by the Vendor. The method and content of the notification of the affected parties will be coordinated with, and is subject to approval by the State, unless required otherwise by legal requirements. If the State decides that the Vendor will be distributing, broadcasting to, or otherwise releasing information on the Security Incident to the news media, the State will decide to whom the information will be sent, and the State must approve the content of any information on the Security Incident before it may be distributed, broadcast, or otherwise released. The Vendor must reimburse the State for any costs associated with the notification, distributing, broadcasting, or otherwise releasing information on the Security Incident.

- A. The Vendor must notify the State contact within 12 hours of the Vendor becoming aware that a Security Incident has occurred. If notification of a Security Incident to the State contact is delayed because it may impede a criminal investigation or jeopardize homeland or federal security, notification must be given to the State within 12 hours after law-enforcement provides permission for the release of information on the Security Incident.
- B. Notification of a Security Incident at a minimum is to consist of the nature of the data exposed, the time the incident occurred, and a general description of the circumstances of the incident. If all of the information is not available for the notification within the specified time period, the Vendor must provide the State with all of the available information along with the reason for the incomplete notification. A delay in excess of 12 hours is acceptable only if it is necessitated by other legal requirements.
- C. At the State's discretion within 12 hours the Vendor must provide to the State all data available including:
 - 1. name of and contact information for the Vendor's Point of Contact for the Security Incident,
 - 2. date and time of the Security Incident,
 - 3. date and time the Security Incident was discovered,
 - 4. description of the Security Incident including the data involved, being as specific as possible,
 - 5. the potential number of records, and if unknown the range of records,
 - 6. address where the Security Incident occurred, and
 - 7. the nature of the technologies involved. If not all of the information is available for the notification within the specified time period, the Vendor must provide the State with all of the available information along with the reason for the incomplete information. A delay in excess of 12 hours is acceptable only if it is necessitated by other legal requirements.
- D. If the Security Incident falls within the scope of South Dakota Codified Law Chapter 22-40, the Vendor is required to comply with South Dakota law.

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

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

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

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

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

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

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

Section XXII. 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 XXIII. 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 XXIV. 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 XXV. Security Acknowledgment Form

The Vendor will be required to sign the Security Acknowledgement Form which is attached to this Agreement as BIT Attachment 2. The signed Security Acknowledgement Form must be submitted to the State and approved by the South Dakota Bureau of Information and Telecommunications and communicated to the Vendor by the State contact before work on the contract may begin. This Security Acknowledgment Form constitutes the agreement of the Vendor to be responsible and liable for ensuring that the Vendor, the Vendor's employee(s), and subcontractor's, agents, assigns and affiliated entities and all of their employee(s), participating in the work will abide by the terms of the Information Technology Security Policy (ITSP) attached to this Agreement. Failure to abide by the requirements of the ITSP or the Security Acknowledgement Form can be considered a breach of this Agreement at the discretion of the State. It is also a breach of this Agreement, at the discretion of the State, if the Vendor does not sign another Security Acknowledgement Form covering any employee(s) and any subcontractor's, agent's, assign's, or affiliated entities' employee(s), any of whom are participating in the work covered by this Agreement, and who begin working under this Agreement after the project has begun. Any disciplining of the Vendor's, Vendor's employee(s), or subcontractor's, agent's, assign's, or affiliated entities' employee(s) due to a failure to abide by the terms of the Security Acknowledgement Form will be done at the discretion of the Vendor or subcontractors, agents, assigns, or affiliated entities and in accordance with the Vendor's or subcontractor's, agent's, assign's, and affiliated entities' personnel policies. Regardless of the actions taken by the Vendor and subcontractors, agents, assigns, and affiliated entities, the State will retain the right to require at the State's discretion the removal of the employee(s) from the project covered by this Agreement.

Section XXVI. Background Investigations

The State requires any person who writes or modifies State-owned software, alters hardware, configures software of State-owned technology resources, has access to source code or protected Personally Identifiable Information (PII) or other confidential information, or has access to secure areas to undergo fingerprint-based background investigations. These fingerprints will be used to check the criminal history records of both the State of South Dakota and the Federal Bureau of Investigation. These background investigations must be performed by the State with support from the State's law enforcement resources. The State will supply the fingerprint cards and prescribe the procedure to be used to process the fingerprint cards. Project plans should allow 2-4 weeks to complete this process.

If work assignments change after the initiation of the project covered by this Agreement so that a new person will be writing or modifying State-owned software, altering hardware, configuring software of State-owned technology resources, have access to source code or protected PII or other confidential information, or have access to secure areas, background investigations must be performed on the individual who will complete any of the referenced tasks. The State reserves the right to require the Vendor to prohibit any person from performing work under this Agreement

whenever the State believes that having the person performing work under this Agreement is detrimental to the project or is considered by the State to be a security risk, based on the results of the background investigation. The State will provide the Vendor with notice of this determination.

Section XXVII. Information Technology Standards

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

Section XXVIII. 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 XXIX. 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.

- 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 XXX. 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 XXXI. 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 XXXII. 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 XXXIII. Web and Mobile Applications

- A. The Vendor's application is required to:

1. have no code or services including web services included in or called by the application unless they provide direct, functional requirements that support the State's business goals for the application,
2. encrypt data in transport and at rest using a mutually agreed upon encryption format,
3. close all connections and close the application at the end of processing,
4. have documentation that is in grammatically complete text for each call and defined variables (i.e., using no abbreviations and using complete sentences) sufficient for a native speaker of English with average programming skills to determine the meaning or intent of what is written without prior knowledge of the application,
5. have no code not required for the functioning of application,
6. have no "back doors", a back door being a means of accessing a computer program that bypasses security mechanisms, or other entries into the application other than those approved by the State,
7. permit no tracking of device user's activities without providing a clear notice to the device user and requiring the device user's active approval before the application captures tracking data,
8. have no connections to any service not required by the functional requirements of the application or defined in the project requirements documentation,
9. fully disclose in the "About" information that is the listing of version information and legal notices, of the connections made, permission(s) required, and the purpose of those connections and permission(s),
10. ask only for those permissions and access rights on the user's device that are required for the defined requirements of the Vendor's application,
11. access no data outside what is defined in the "About" information for the Vendor's application,
12. conform to Web Content Accessibility Guidelines 2.0,
13. have Single Sign On capabilities with the State's identity provider and
14. any application to be used on a mobile device must be password protected.

B. The Vendor is required to disclose all:

- A. functionality,
- B. device and functional dependencies,
- C. third party libraries used,
- D. methods user data is being stored, processed, or transmitted,
- E. methods used to notify the user how their data is being stored, processed, or transmitted,
- F. positive actions required by the user to give permission for their data to be stored, processed and or transmitted,
- G. methods used to record the user's response(s) to the notification that their data is being stored, processed, or transmitted,
- H. methods used to secure the data in storage, processing, or transmission,
- I. forms of authentication required for a user to access the application or any data it gathers stores, processes and or transmits,
- J. methods used to create and customize existing reports,
- K. methods used to integrate with external data sources,
- L. methods used if integrates with public cloud provider,
- M. methods and techniques used and the security features that protect data, if a public cloud provider is used, and
- N. formats the data and information uses.

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 XXXIV. 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 XXXV. 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 XXXVI. Vendor Training Requirements

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

- A. legal requirements for handling data,
- B. media sanitation,
- C. strong password protection,
- D. social engineering, or the psychological manipulation of persons into performing actions that are inconsistent with security practices or that cause the divulging of confidential information, and
- E. security incident response.

Section XXXVII. Data Sanitization

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

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

Section XXXVIII. 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 XXXIX. 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 XL. 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 XLI. Rights, Use, and License of and to State Data

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

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

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

Section XLII. 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 XLIII. 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 XLIV. 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 XLV. 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 XLVI. Scanning and Audit Authorization

The Vendor will provide the State at no cost and at a date, time, and for duration agreeable to both parties, authorization to scan and access to a test system containing test data for security scanning activities. The system and data provided to the State by the Vendor for testing purposes will be considered a test system containing test data. The State will not scan any environment known by the State to be a production environment at the time the scan is performed by the State. The Vendor provides their consent for the State or any third-party acting for the State to scan the systems and data provided as the State wishes using any methodology that the State wishes. Any scanning performed by the State will not be considered a violation of any licensure agreements the State has with the Vendor or that the Vendor has with a third-party.

The Vendor will also allow the State at the State's expense, not to include the Vendor's expenses, to perform up to two security audit and vulnerability assessments per year to provide verification of the Vendor's IT security safeguards for the system and its data. The State will work with the Vendor to arrange the audit at a time least likely to create workload issues for the Vendor and will accept scanning a test or UAT environment on which the code and systems are a mirror image of the production environment.

Scanning by the State or any third-party acting for the State will not be considered reverse engineering. If the State's security scans discover security issues the State may collaborate, at the State's discretion with, the Vendor on remediation efforts. These remediation efforts will not be considered a violation of any licensure agreements between the State and the Vendor. In the event of conflicting language, this clause supersedes any other language in this, or any other agreement made between the State and the Vendor.

The Vendor agrees to work with the State to rectify any serious security issues revealed by the security audit or security scanning. This includes additional security audits and security scanning that must be performed after any remediation efforts to confirm the security issues have been resolved and no further security issues exist. If the Vendor and the State agree that scanning

results cannot be achieved that are acceptable to the State, then the State may terminate the Agreement without further obligation.

Section XLVII. 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 XLVIII. Movement of Protected State Data

Any State Data that is protected by federal or state statute or requirements or by industry standards must be kept secure. When protected State Data is moved to any of the Vendor's production or non-production systems, security must be maintained. The Vendor will ensure that that data will at least have the same level of security as it had on the State's environment.

Section XLIX. Banned Services

The Vendor warrants that any hardware or hardware components used to provide the services covered by this Agreement were not manufactured by Huawei Technologies Company or ZTE Corporation, or any subsidiary or affiliate of such entities. Any company considered to be a security risk by the government of the United States under the International Emergency Economic Powers Act or in a United States appropriation bill will be included in this ban.

Section L. 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 D – Information Technology Security Policy (ITSP) - Contractor

The winning vendor will be required to follow the security policies laid out by the State's Bureau of Information and Telecommunications as described in the Information Technology Security Policy (ITSP) - Contractor. This document can be downloaded from the procurement website as ***SDDOT Construction Management System-ITSP-Contractor-Appendix D-24RFP9741.pdf***

Do not include a copy of this in your response.

Appendix E – Security Acknowledgement form

The winning vendor will be required to return this form as part of the contract. It is presented here for information only and should **NOT** be signed or returned with your proposal.

 <small>south dakota Bureau of Information & Telecommunications</small>	<hr/> Security Acknowledgement <hr/>	 <small>SOUTH DAKOTA CYBER SECURITY</small>
Please return agreement to your BIT Manager or Designated BIT Contact		
<p>All BIT employees and State contractors must sign; Agreement to Comply with BIT Information Technology Security Policy (the "Policy"). Users are responsible for compliance to all information security policies and procedures. <u>By signature below, the employee or contractor hereby acknowledges and agrees to the following:</u></p> <ol style="list-style-type: none">1. Employee is a State of South Dakota employee or contractor that uses non-public State of South Dakota technology infrastructure or information;2. Employee or contractor will protect technology assets of the State from unauthorized activities including disclosure, modification, deletion, and usage;3. Employee or contractor agrees to follow state and federal regulations in regards to confidentiality and handling of data;4. Employee or contractor has read and agrees to abide by the Policy;5. Employee or contractor consents to discuss with a supervisor / State contact regarding Policy violations;6. Employee or contractor shall abide by the policies described as a condition of continued employment / service;7. Employee or contractor understands that any individual found to violate the Policy is subject to disciplinary action, including but not limited to, privilege revocation, employment termination or financial reimbursement to the State;8. Access to the technology infrastructure of the State is a privilege which may be changed or revoked at the discretion of BIT management;9. Access to the technology infrastructure of the State automatically terminates upon departure from the State of South Dakota employment or contract termination;10. Employee or contractor shall promptly report violations of security policies to a BIT manager or State Contact and BIT Help Desk (605.773.4357);11. The Policy may be amended from time to time. The State of South Dakota recommends employees and contractors for the State to regularly review the appropriate Policy and annual amendments. <p><i>Information Technology Security Policy – BIT:</i> http://intranet.bit.sd.gov/policies/ <i>Information Technology Security Policy – CLIENT:</i> http://intranet.bit.sd.gov/policies/ <i>Information Technology Security Policy – CONTRACTOR:</i> http://bit.sd.gov/vendor/default.aspx</p>		
<p>Acknowledgement: State of South Dakota Information Technology Security Policy</p> <p>Contractor: If the individual is signing for their entire company by signing this form the individual affirms that they have the authority to commit their entire organization and all its employees to follow the terms of this agreement.</p>		
<div style="display: flex; align-items: center; justify-content: space-between;"><div style="border: 2px solid blue; padding: 5px; font-weight: bold; color: blue; font-size: 1.2em;">DRAFT</div><div style="display: flex; width: 100%;"><div style="border-bottom: 1px solid black; width: 30%;"></div><div style="border-bottom: 1px solid black; width: 30%;"></div><div style="border-bottom: 1px solid black; width: 30%;"></div><div style="border-bottom: 1px solid black; width: 30%;"></div></div><div style="display: flex; justify-content: space-between; margin-top: 5px;">Employee or Contractor signatureDateBIT Manager or ContactDate</div></div>		
<div style="border-bottom: 1px solid black; height: 1.2em; margin-bottom: 5px;"></div> <p>Employee or Contractor name and Company name in block capital letters</p>		