STATE OF SOUTH DAKOTA

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

COMPUTERIZED CRIMINAL HISTORY (CCH)
PROPOSALS ARE DUE NO LATER THAN October 1, 2021

Amended 06/30/2021
Section 2.0 – Databases
Section 5.0
Section 5.6.23

RFP #: 2316   BUYER: South Dakota Division of Criminal Investigation (SD DCI),
Division of Criminal Investigation (DCI)
EMAIL: RFP2316@state.sd.us

READ CAREFULLY

FIRM NAME:	AUTHORIZED SIGNATURE:
ADDRESS:	TYPE OR PRINT NAME:
CITY/STATE:	TELEPHONE NO:
ZIP (9 DIGITS):	FAX NO:
FEDERAL TAX ID#:	E-MAIL:

PRIMARY CONTACT INFORMATION

CONTACT NAME:	TELEPHONE NO:
FAX NO:	E-MAIL:

1.0 GENERAL INFORMATION

1.1 Standard Contract Terms and Conditions

Any contract or agreement resulting from this RFP will include the SD DCI's standard contract terms listed in Appendix A, along with any additional contract terms as negotiated by the parties. As part of the negotiation process the contract terms listed in Appendix B may be altered or deleted. The Offeror should indicate in their response any issues they have with specific contract terms if the Offeror does not indicate that there are any issues with any contract terms then SD DCI will assume those terms are acceptable to the Offeror.

1.2 BIT Standard Contract Terms and Conditions

Any contract or agreement resulting from this RFP will include the State's standard I/T contract terms listed in Appendix B for a State Hosted Proposal along with any additional contract terms as negotiated by the parties. As part of the negotiation process the contract terms listed in Appendix B may be altered or deleted. The Offeror should indicate in their response any issues they have 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 C. These questions must be answered and may be used in the proposal evaluation.

1.3 Purpose for Request Proposal (RFP)

1.3.1 Background: The South Dakota Division of Criminal Investigation (SD DCI), under the South Dakota Office of the Attorney General, is looking for a new CCH to replace their current system, due to certain limitations of the current system.

1.3.2 Goals and Objectives: The SD DCI would like to replace the current CCH with a new system. We are looking for a solution that will include all current functionality, as well as solve issues we have with our current system. The main issues we are looking to address include the need for highly accurate search functionality and the ability to merge missing dispositions received from the Unified Judicial System's Odyssey software. The SD DCI would give preference to a vendor who has past CCH development experience.

1.3.3 Description of Components or Phases: The SD DCI is looking for a CCH solution that is used in other agencies and has proven functionality and usability, with the ability to be custom programmed for any additional South Dakota needs. This solution can be application or web based. It will need to be hosted on the South Dakota State infrastructure and should have the ability to integrate with the State's Azure Active Directory to control user authentication and access.

As part of the State's Identity and Access Management (IAM) strategy, the proposed system will need to integrate with the State of South Dakota's standard identity management service (SSO) which enables custom control of how citizens sign up, sign in, and manage their profiles. The SSO supports two industry standard protocols: OpenID Connect and OAuth 2.0. This identity management will handle password recovery. Multi-factor Authentication (MFA) is required for all application Administrators and may be required for other users.

This project is solely dependent on the availability of appropriated funding, grant approvals and

timelines, as well as expenditure authority from the Legislature for this purpose in the next fiscal year.

1.3.4 Scope of components or Phases: The four phases are expected to have the following components:

1.3.4.1 Phase one will include the following
1.3.4.1.1 Award the RFP
1.3.4.1.2 Negotiate and sign the contract
1.3.4.1.3 Kick off meeting, which can be either remotely or onsite, depending on the COVID-19 situation at that time. This meeting will include all project staff, technical support, and end user representation
1.3.4.1.4 Establish initial project timeline and project plan
1.3.4.1.5 Establish team assignments
1.3.4.1.6 Finalize solution requirements
1.3.4.1.7 Establish testing and exercise requirements including identifying external testing agencies
1.3.4.1.8 Establish the time the system needs to operate trouble free for final acceptance
1.3.4.2 Phase two will include the following:
1.3.4.2.1 Customize the product as needed
1.3.4.2.2 Set up the test system
1.3.4.2.3 Integration testing
1.3.4.2.4 Functional testing
1.3.4.2.5 Performance testing
1.3.4.2.6 Load testing
1.3.4.2.7 Completion of security requirements (As agreed in the final contract)
1.3.4.3 Phase three testing will include the following:
1.3.4.3.1 UAT testing
1.3.4.3.2 Training remote or onsite, depending on the COVID-19 situation at that time
1.3.4.4 Phase four will include the following:
1.3.4.4.1 System Go Live
1.3.4.4.2 Resolution of any problems found
1.3.4.4.3 Additional training as needed
1.3.4.4.4 Allow system to operate trouble free for a predetermined period of time

The proposal may include a project plan with different phases, but any project plan must include as a minimum the items list above. Deviation from the phases listed above should be explained as stated in 7.5. Completion of the final item in each phase will be the milestone for that phase. Payment will be based on the successful completion of each milestone. The percentage paid for each completed phase is negotiable.

1.4 Issuing Office and RFP Reference Number

The SD DCI is the issuing office for this document and all subsequent addenda relating to it, on behalf of the State of South Dakota and the SD Office of the Attorney General (ATG). The reference number for the transaction is RFP2316@state.sd.us. This number must be referred to on all proposals, correspondence, and documentation relating to the RFP.

1.5 Scheduling of Activities (Subject to Change)

1.6 Submitting Your Proposal

All proposals must be completed and received by SD DCI by the date and time indicated in the Schedule of Activities.

Proposals received after the deadline will be ineligible for consideration. An original and 6 identical copies of the proposal shall be submitted. Also, Offerors are required to provide an electronic copy of their response on a flash drive. The electronic copy should be provided in MS WORD or in PDF format, except for the project plan, which must be in MS Project or MS Excel.

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

> **REQUEST FOR PROPOSAL #2316**
> **PROPOSAL TITLE CCH RFP**
> **DUE: October 1, 2021**
> **BUYER: South Dakota Attorney General's Office**
> **Attention: CCH RFP #2316**
>   **Jamie Reed**
> **Address: 1302 E Hwy 14, Suite 5**
>   **Pierre, SD 57501-8505**

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

1.7 Certification Regarding Department, Suspension, Ineligibility and Voluntary Exclusion – Lower Tier Covered Transactions

By signing and submitting this proposal, the Offeror certifies that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation, by any Federal department or agency, from transactions involving the use of Federal funds.

Where the Offeror is unable to certify to any of the Statements in this certification, the bidder shall attach an explanation to their offer.

1.8 Non-Discrimination Statement

The State of South Dakota requires that all 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 regards to race, color, creed, religion, age, sex, ancestry, national origin or disability.

1.9 Modification or Withdrawal of Proposals

Proposals may be modified or withdrawn by the Offeror prior to the established due date and time.

No oral, telephonic, telegraphic or facsimile responses or modifications to informal, formal bids, or Request for Proposals will be considered.

1.10 Offeror Inquiries

All questions should be sent to: RFP2316@state.sd.us, only emailed questions will be accepted.

Offeror may submit email questions concerning this RFP to obtain clarification of requirements. No questions will be accepted after the date and time indicated in the schedule of activities. Email questions to the email address listed above must contain in the subject line "RFP #2316". The questions and their answers will be posted on the ATG Website at http://atg.sd.gov/OurOffice/rfp.aspx before the proposal submittal date and will be posted by the date and time indicated in the calendar of events. Offeror may not rely on any other statements, either of a written or oral nature, that alter any specification or other term or condition of this RFP that have not originated from the SD RFP Project Contact. Offerors will be notified in the same manner as indicated above regarding any modifications to this RFP.

1.11 Proprietary Information

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

1.12 Length Of Contract

The contract will begin on July 1, 2022.
The contract will end on June 30, 2023.
If first year maintenance is included in the proposal, contract end date will be negotiable.

The State in its sole discretion may renew the Agreement under the same terms and conditions for up to four (4) additional one-year periods. Offerors understand that ANY award of the contemplated contract is subject to the approval and availability of funds.

1.13 Site Visit

If site visits are required, SD DCI will first determine if a site visit is an option, due to the SD Covid situation at that time. If deemed allowable, the site visit will be scheduled before the submission of the proposal. Site visits will be made at the Offeror's expense.

1.14 Presentations/Demonstrations

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

1.15 Discussions

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

1.16 Negotiations

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

1.17 Restriction of Boycott of Israel

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

The bidder in preparing its response in considering bids 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, 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 submitted by the bidder on this project and terminate any contract awarded based on the bid. The successful bidder 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.

2.0 SCOPE OF WORK

Offender Management
Display a list of all offenders in the system
Search and filter offenders using information found in the offender record
Select an offender automatically if there is only one search or filter result
Display personal descriptor, alias, and arrest information for a selected offender
Display charge and disposition information for an arrest of a selected offender
Update personal descriptor, alias, and arrest information for a selected offender
Update charge and disposition information for an arrest of a selected offender
Add a new offender to the system
Add a new alias or arrest to a selected offender
Add a new charge or disposition to an arrest of a selected offender
Delete an offender and any associated aliases, arrests, charges, and dispositions
Delete an alias from a selected offender
Delete an arrest and any associated arrests and dispositions
Delete arrests and dispositions from an arrest of a selected offender
Seal an alias for a selected offender
Seal an arrest and any associated arrests and dispositions
Seal a charge or disposition for an arrest of a selected offender
Unseal an alias for a selected offender
Unseal an arrest and any associated arrests and dispositions
Unseal a charge or disposition for an arrest of a selected offender
Consolidate one offender into another by filling in missing information from one into the other
Consolidate aliases for an offender by combining them, removing any duplicates
Consolidate arrests for offender by combining them, ignoring duplicates
Record who or what last updated an offender record, including the section that was updated and when the update occurred
Toggle between read-only and edit modes on the form
Agency (ORI) Management
Display a list of all agencies in the system
Search and filter agencies using information found in the agency record
Select an agency automatically if there is only search or filter result
Display information for a selected agency

Update information for a selected agency
Add a new agency to the system
Record who or what last updated an agency record, including when the update occurred
Toggle between read-only and edit modes on the form

Charge Code Management

Display a list of all charge codes in the system
Search and filter charge codes using information found in the charge code record
Search and filter charge codes using UJS codes
Select a charge code automatically if there is only search or filter result
Display general and UJS code information for a selected charge code
Update general and UJS code information for a selected charge code
Add a new charge code to the system
Add a new UJS code to a selected charge code
Record who or what last updated a charge code record, including the section that was updated and when the update occurred
Toggle between read-only and edit modes on the form

Audit and Change Logging

Display a list of all recorded changes to data in the system
Search and filter record changes to data in the system

Interfaces

AFIS

CCH receives description and arrest information and updates or adds history as needed
Afis would update SID assigned by CCH if no SID exists in AFIS

NCIC

Return CCH information to NCIC through a query request
NCIC sends CCH Single/Multi source indicator and assigned FBI #s. CCH then updates the record appropriately

UJS/ODYSSEY Merge Correction Queue

Display a list of all failed ODYSSEY merges
Display information for a selected failed merge
Display a proposed correction for a selected failed merge
Accept a correction and merge it with the offender record
Reject a correction
Record the merge attempt and whether it succeeded, failed, corrected, or rejected

Reporting

List of arrests over a year old that have no dispositions
List of queries made on offenders through NCIC

Database

Design and implement new database structure
~~Export data from mainframe system database~~
~~Import data from mainframe system database~~
Ability to import data from SQL Server 13.0.5865.1
Ability to import old mainframe data that is located in current sql database
User Management
Azure Active Directory B2C (Azure AD B2C) interface for user account management
Multiple roles (search only, view/read only, full access)
Project Management & Security Related Tasks
Meetings
Navigation and design
Testing and bug fixes
Project management and documentation
Security scanning and fixes
test and production environment setup
Training
Manual
Tooltips

3.0 RESOURCES

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

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

3.1. Team Organization: Provide the following information.
3.1.1 Project Organization Chart
List names, job titles (designate vacancies), and the city and state in which individual will work on this project.

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

3.2 Project Staffing Roles

<u>Agency Project Sponsor</u>
Agency DCI Assistant Director

Role: Some of the duties performed by the Agency Project Sponsor are:
- Resolves resource and priority conflicts
- Holds subordinate managers accountable for their performance
- Has a direct communications and reporting relationship with the Agency Project Manager, Agency IT Team Leader

Agency Project Manager
Identification Supervisor

Role: Some of the duties performed by the Agency Project Manager are:
- Keeps the team focused on appropriate goals
- Approves the Project Plan
- Holds the project team accountable for planning and executing the project
- Holds the team accountable for delivering agreed-upon results
- Approves vendor payments based on contract/work order language
- Day to day oversight of the project
- Is the chief advocate for the project
- Has direct communication and reporting relationship with Agency IT Team Leader and Agency IT Project Leader

Reports to: The Agency Project Sponsor and Agency Project Manager.

Agency IT Team Leader
IT Administrator

Role: Some of the duties of the Agency IT Team Leader are:
- Day to day oversight of the project technical specifications
- Main contact with vendor regarding project contract
- Approves vendor payments based on contract/work order language
- Able to advise the Agency Project Manager and Agency IT Project Leader of cost/benefit as well as consequences of any changes in work direction

Reports to: Agency Project Sponsor

Agency IT Project Leader
IT Technology Engineer

Role: Some of the duties of the Agency IT Team Leader are:
- Day to day oversight of the project technical specifications
- Main contact with vendor regarding project status and progress
- Keeps the team updated with new information
- In close daily contact with Agency Project manager to ensure that all requirements are fulfilled
- Consult with Agency IT Team Leader on any project issues, concerns or conflicts that may arise

- Able to advise the Agency Project Manager and Agency IT Team Leader of cost/benefit as well as consequences of any changes in work direction

Reports to: Agency Project Sponsor and Agency IT Team Leader

Project Steering Team
    ATG IT Staff
    ATG Fiscal Staff
    DCI Identification Section
    BIT Agency POC
Role: Some of the duties performed by the Project Steering Team:

- Oversee the project in terms of the contract and work order agreements. Specific items of oversight include:
  - What are the deliverables for his or her agency, and are they being met?
  - Is the project on schedule? If not, what are the consequences? Should the project be put back on schedule and how will that be done?
  - What expenditures have been made? Is the project on budget? If not, what are the circumstances surrounding it?
- Recommendation of approval of any scope changes, or any changes that affect cost and schedule based on cost benefit to the Project Owner

Reports to: Agency Project Manager

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

3.3 Staff Resumes and References

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

- Name
- Title
- Contact Information (telephone number(s), e-mail address)
- Work Address
- Project Responsibilities (as they pertain to this project)
- Percentage of time designated to this project
- Brief listing of Work Experience in reverse chronological order from present to January, 2012 (only provide company name, job title(s)/position(s) held, date started and date left each position, brief description of job duties, responsibilities, and significant accomplishments)
- RFP Project Experience
- Technical Background relative to this project

- Experience in Similar Projects
- Names of the Similar Projects they were involved in
- Role they played in the projects similar to this project
- Project Management Experience
- Technical Knowledge
- Education
- Relevant Certifications
- Three Professional References (name, telephone number, company name, relationship to employee)

4.0 PROJECT DELIVERABLES/APPROACH/METHODOLOGY

The Offeror is required to include a test system for Offeror's application. This test system will be used at the discretion of the State to test functionality before it is deployed to Production. All resource costs associated with keeping the test system available must be borne by the Offeror. Any licensing costs for the test system must be included with the cost proposal.

At the State'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 the States' discretion if the code changes are applied by the State or the Offeror. If the code testing delays a project's timeline a change management process should be followed, and SD DCI will not be charged for delay and/or impact to the timeline. 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 the State. Testing of emergency code changes will be scheduled by the State based on the severity and resource availability.

The test system will be maintained by the Offeror as a mirror image of the production system code base. At the State'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.

Data in the test system must not contain valid PII, PHI, FTI or other secure, factual information. If copying data from a production environment, data must be de-identified, falsified, and/or otherwise altered such that it is no longer protected under state or federal law before being loaded into a test system.

The Agreement associated with this project will also be an Agreement for the State to own the data tables and be able to manipulate data, run reports as needed, pull code tables, access raw data and develop dashboards as needed through Microsoft Power BI, ESRI, Tableau and associated platforms.

As part of the State's Identity and Access Management (IAM) strategy, the proposed system 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 State employees and citizens sign up, sign in, and manage their profiles.

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

5.0 FORMAT OF SUBMISSION

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

Offerors are required to provide an electronic copy of their response. The electronic copy should be provided in MS WORD or in PDF format, except for the project plan, which must be in MS Project or MS Excel. The submission must be delivered as indicated in Section 1.7 of this document.

The Offeror is cautioned that it is the Offeror's sole responsibility to submit information related to the evaluation categories and that the State of South Dakota is under no obligation to solicit such information if it is not included with the proposal. The Offeror's failure to submit such information may cause an adverse impact on the evaluation of the proposal. You should respond to each point in the Scope of Work and Deliverables in the order they were presented.

Offerors and their agents (including subcontractors, employees, vendors, or anyone else acting on their behalf) must direct all their questions or comments regarding the RFP, the evaluation, etc. to
SD DCI
Attn: ~~Background Check Payment Website~~ CCH
RFP #2316
Jamie Reed.

Offerors and their agents may not contact any state employee other than the SD DCI office at RFP2316@state.sd.us regarding any of these matters during the solicitation and evaluation process. Inappropriate contacts are grounds for suspension and/or exclusion from specific procurements. Offerors and their agents who have questions regarding this matter should contact the SD DCI office at RFP2316@state.sd.us.

The Offeror may be required to submit a copy of their most recent audited financial statements upon SD DCI's request.

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

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

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

> 5.1 Executive Summary
> 5.2 Statement of Understanding of Project
> 5.3 Corporate Qualifications

5.4 Relevant Project Experience

5.5 Project Plan

5.6 Deliverables

5.7   Non-Standard Software and Hardware

5.8   System Diagram (if not a separate document)

5.9   Security and Vendor Questions (if not a separate document)

5.10 Notation of any issues with the State's contract terms (Appendix B)

5.1 Executive Summary

A one or two page executive summary that briefly describes the vendor's proposal. This summary should highlight the major features of the proposal. It must indicate any requirements that cannot be met by the vendor. The reader should be able to determine the essence of the proposal by reading the executive summary. Proprietary information requests should be identified in this section.

5.2 Statement of Understanding of Project

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

5.3 Corporate Qualifications

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

A. What year was your parent company (if applicable) established?

B. What is the business of your parent company?

C. What is the total number of employees in the parent company?

D. What are the total revenues of your parent company?

E. How many employees of your parent company have the skill set to support this effort?

F. How many of those employees are accessible to your organization for active support?

G. What year was your firm established?

H. Has your firm ever done business under a different name and if so what was the name?

I. How many employees does your firm have?

J. How many employees in your firm are involved in this type of project?

K. How many of those employees are involved in on-site project work?

L. What percent of your parent company's revenue (if applicable), is produced by your firm?

M. Corporate resources available to perform the work, including any specialized services, within the specified time limits for the project.

N. Availability to the project locale.

O. Familiarity with the project locale.

P. Has your firm ever done business with other governmental agencies? If so, please provide references.

Q. Has your firm ever done business with the State of South Dakota? If so, please provide references.

R. Has your firm ever done projects that are like or similar to this project? If so, how many clients are using your solution? Please provide a list of four or more locations of the same approximant nature as SD DCI where your application is in use along with contact names and numbers for those sites. The State of South Dakota has a consolidated IT system. **Either** any references given should be from States with a consolidated IT system, to be acceptable **or** the reference should be a detailed explanation on how you will modify your work plan for a consolidated environment that you are unfamiliar with.

S. Provide the reports of third-party security scans done at the end of the four projects you provided in your proposal response. If there are no audits of these projects then provide, unedited and un-redacted results of such security testing/scanning from third-party companies and/or tools that has been run within the past 90 days. The State will sign a non-disclosure agreement, as needed, redaction of these scan reports can be done within the limits of the State's open records law.

T. What is your Company's web site?

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

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

5.4 Relevant Project Experience

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

quality of the work and the total of what the Offeror accomplished in the project.

A. Client/Company Name

B. Client Company Address, including City, State and Zip Code

C. Client/Company Contacts(s)

> Name
> Title
> Telephone Number
> E-mail address
> Fax Number

D. Project Start Date

E. Project Completion Date

F. Project Description and Goals

G. Offeror's Role in Project

H. Offeror's responsibilities

I. Offeror's Accomplishments

J. Description of How Project Was Managed

K. Description of Price and Cost Data from Project

L. Description of special project constraints, if applicable

M. <u>Description of your ability and proven history in handling special project constraints</u>

N. Description of All Changes to the Original Plan or Contract That Were Requested

O. Description of All Changes to the Original Plan or Contract That Offeror Completed

P. Description of How Change Requests Were Addressed or Completed by Offeror

Q. Was Project Completed in a Timeframe That Was According to the Original Plan or Contact? (If "No", provide explanation)

R. Was Project Completed Within Original Proposed Budget? (If "No" provide explanation)

S. Was there any Litigation or Adverse Contract Action regarding Contract Performance? (If "Yes" provide explanation)

T. Feedback on Offeror's Work by Company/Client

U. Offeror's Statement of Permission for the Department to Contact the Client/Company and for the Client's/Company's Contract(s) to Release Information to the Department

5.5 Project Plan

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

- <u>Proposed project management techniques</u>

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

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

If as part of this project, the Offeror plans to set-up or configure the software and/or hardware and plans to do this outside of South Dakota, even in part, then they need to provide a complete and detailed project plan on how the Offeror plans on migrating to SD DCI's site. Failure to do this is sufficient grounds to disregard the submission, as it demonstrates that the Offeror fundamentally does not understand the project. Providing a work plan for the steps above that is complete and detailed maybe sufficient.

5.6 Deliverables

This section should constitute the major portion of the work to be performed. Provide a complete narrative detailing the assessment of the work to be performed, approach and methods to provide the requirements of this RFP, the Offeror's ability to fulfill the requirements of this RFP, the Offeror's approach, the resources necessary to fulfill the requirements, project management techniques, specialized services, availability to the project locale, familiarity with the project locale and a description of any options or alternatives proposed. This should demonstrate that the Offeror understands the desired overall performance expectations. This response should identify each requirement being addressed as enumerated in section 5.0. If you have an alternative methodology or deliverables you would like to propose, please include a detailed description of the alternative methodology or deliverables and how they will meet or exceed the essential requirements of the methodology and deliverables described in Section 4.0.

5.6.1 The Vendor shall develop design documents to include the technical architecture and system design of the application. This documentation shall contain the architectural diagrams as well as system configuration and any custom development to the application. The documentation shall be detailed enough for reviewers to understand the function and appearance of all screens.

5.6.2 Interfaces — The Vendor shall be responsible for implementing all aspects of the interfaces described in the Technical Requirements. The Vendor shall be responsible for working with the Agency Project Manager and Agency IT Project Manager to understand the technical interface requirements.

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

capability shall be included in the Proposal.

5.6.3 Hardware — If a state hosted solution is proposed, upon award, the Vendor shall work with the SD DCI and SD BIT to understand the existing infrastructure, assess hardware and software compatibility, and gather information on licenses available for use on this project. The findings of these examinations shall be compiled by the Vendor and submitted to the Agency Project Manager. All Vendor warranty and licensing agreements associated with this system shall be in the name of the SD DCI. The Vendor shall install, test and commission all software required to support the system.

LLEAs shall be responsible for providing user workstations. SD DCI/BIT shall discuss any suggested network enhancements. The Vendor's responsibilities are limited to suggesting the improvements to network infrastructure during proposal submission and as a result of the design efforts.

5.6.4 Acquisition of third-party applications or data bases for RFPS. The acquisition of any third-party software, hardware or databases needed to fulfil the project's contract requires the active participation of the State. The State must approve the costs as well as the terms and conditions of the acquisition of each individual item. The terms and conditions of the acquisition of any open source or freeware software must be also be approved by the State before acquisition. Project plans should allow sufficient time for the acquisition process.

5.6.5 Application Software Code — Preference will be given to Vendor solutions which deliver all application software code to SD DCI in an acceptable format (DVD, tape, ftp site, etc.).

5.6.6 Technical Documentation — If proposing State hosted solution, System and Technical Documentation sufficient for SD DCI IT to maintain and support the system shall be provided by the selected Vendor, including documentation for the software application, data repository, data interfaces, network etc.

5.6.7 Detailed Project Schedule and milestones with delivery dates showing sub-projects activities and tasks, milestones and targeted delivery data and resources required and allocated to each. The Project Schedule shall be updated on a weekly basis in MS Project or MS excel and submitted to the Agency Project Manager and Agency IT Project Manager.

5.6.8 Plan of Work — a subordinate document made following establishment of a contract with the awarded Vendor and acceptance of a Project Management Plan. One or more SOWs may be used to provide specific details regarding migration, testing, acceptance and related project work, but may not modify the terms of the contract.

5.6.9 Weekly Status/ Progress Reports that reflect the current status of each active project task, projection of work to be performed the next week, alerts of potential problems and schedule delays and risk mitigation plans.

5.6.10 The Vendor's organization chart and staffing table with names and title of personnel assigned to the project. This shall be in agreement with consistent staffing of accepted proposal. Necessary substitutions due to change of employment status and other unforeseen circumstances may only be made with prior approval of SD DCI. Resumes shall be included with the organizational chart for all

Vendor staff assigned to the project.

5.6.11 Each project milestone shall have individual Acceptance Criteria which detail the completion of the specific milestone. The Acceptance Criteria are to be mutually developed by the Agency and the awarded Vendor and documented within forty-five (45) days after the contract award. Vendor payments shall be made pursuant to the Payment Plan that corresponds to each completed milestone as negotiated between the parties.

5.6.12 Communications Plan including contact list, meetings, document distributions, reports, etc.

5.6.13 Issue & Risk Management Plans and Logs—documented plans for logging and managing issues and risks, as well as the associated tracking logs jointly maintained by the Vendor and SD DCI Project Manager, to be reviewed / updated weekly.

5.6.14 Action Item Log — tracking all open project related action items, assignments and due dates jointly maintained by the Vendor and SD DCI Project Manager, to be reviewed / updated weekly.

5.6.15 Staffing and Resource Management Plan — indicates people, system, and network resources required for this procurement by month. This plan shall cover both Vendor and SD DCI/BIT resources.

5.6.16 Configuration Management Plan — describing the version control methodology that shall be in place to manage documentation versions and software releases.

5.6.17 Change Management Plan and a change control board (CCB) comprised of the Vendor, the Development Team Project Manager, the Agency Project Sponsor or Assistant, the Agency IT Project Manager and the Agency Project Manager, are jointly to decide on any changes to this project, pursuant to a mutually agreeable change process that shall be set out as part of the project plan. The CCB shall meet on an ad hoc basis when changes are necessary to the project and, if needed, to the contract. The RFP terms and conditions shall be followed when implementing any changes to the contract, including any necessary State Procurement approvals.

5.6.18 Test Plans - including Integration Testing, User Acceptance Testing, Load Testing and documented test results. Vendor shall recommend specific test levels and structured test environment required for this contract for SD DCI's approval.

5.6.19 Acceptance Plan shall define the process to be followed and criteria for acceptance of each milestone and deliverable. The Acceptance Plan shall include the following elements: Introduction (including the purpose of the Acceptance Plan, Scope, Definitions, References, and Overview), Roles and Responsibilities, Acceptance Tasks, Criteria for Milestones and Deliverables (Section 6), Problem Resolution and Corrective Action, Acceptance Environment and Deliverable/Service Acceptance.

5.6.20 Payment Plan - payment to the awarded Vendor shall be upon the completion and acceptance by SD DCI of each milestone as defined in the project schedule pursuant to Section 6.0, and Payment Terms. The value of each milestone shall be established in the Vendor's Cost Proposal and negotiated and agreed upon during the contract negotiations phase. Any payment change request shall require submission to and approval of SD DCI. The Vendor shall provide an annual payment plan for the life of

this contract if requested by SD DCI.

5.6.21 Quality Management Plan describes the Vendor's method of testing the system and ensuring defects are identified and resolved. Upon award of contract, the Vendor and SD DCI Project Manager shall create the quality management plan together as part of the project management plan development stage. The final version shall be accepted by the Agency in writing before Vendor may proceed with implementation of the Contract. The quality management methodology that shall be used in this Contract shall be included in the Quality Management Plan.

5.6.22 Implementation Plan — describes how the Vendor's solution shall be deployed, installed and transitioned into an operational system. The plan contains an overview of the system, a brief description of the major tasks involved in the implementation, the overall resources needed to support the implementation effort (such as hardware, software, facilities, materials, and personnel), and any site-specific implementation requirements. The implementation schedule shall be mutually agreed upon and set between SD DCI and the Vendor.

5.6.23 Disaster Recovery Plan — Vendor shall meet state hosted standards, this will be provided by BIT. A disaster recovery plan for the ~~Background Check Payment Website~~ CCH should have a Recovery Point Objective of no more than 24 hours.

5.7 Non-Standard Software and Hardware

State standard hardware and software should be utilized unless there is a reason not to. If your proposal will use non-standard hardware and/or software you must first obtain State approval. If your proposal recommends using non- standard hardware and 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 and/or software requires use of the Moratorium Process if the solution is hosted by the State. This process can be found through the Standards' page and must be performed by State employees. The costs of such non-standard software or hardware should be reflected in your cost proposal. The work plan should also account for the time need to use the Moratorium Process. See http://bit.sd.gov/standards/, for lists of the State's standards. The proposal should also include a link to your hardware and software specifications.

If non-standard software and or hardware are used the project plan and the costs stated in 5.6 will have to 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 should also be stated. The project plan should also include the development and implementation of a disaster recovery plan since non-standard software and hardware will not be covered by the State's disaster recovery plan. This should also be reflected in the costs.

There is also a list of technical questions, Security and Vendor Questions which is attached as Appendix C. These questions must be answered and signed by the Offeror and may be used in the proposal evaluation.

6.0 COST PROPOSAL

Offerors may submit multiple cost proposals. All costs related to the provision of the required services

must be included in each cost proposal offered.

Cost will be evaluated as part of the technical proposal. Offerors may submit multiple costs in their proposal.

All costs related to the provision of the required services must be included in each proposal offered.

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

6.1 Staffing

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

6.2 Travel and Expenditure Table

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

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

NOTE: SD DCI asks that vendors accept state per diem. Lodging per diem is $75/night plus tax. Food per

diem is $40/day.

6.3 Other Costs

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

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

6.4 Additional Work

The Offeror may be expected to perform additional work as required by any of SD DCI signatories to a contract. This work can be made a requirement by SD DCI for allowing the application to go into production. This additional work will not be considered a project change chargeable to SD DCI if it is for reasons of correcting security deficiencies, meeting the functional requirements established for the application, unsupported third party technologies or excessive resource consumption. The cost for additional work should be included in your proposal.

7.0 PROPOSAL EVALUATION AND AWARD PROCESS

7.1

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

7.1.1 Specialized expertise, capabilities and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements.

Project Plan
7.1.1.1 Application software functionality
7.1.1.2 Training and documentation Options
7.1.1.3 Warranty and maintenance terms and tiers
7.1.1.4 Customer Service options

7.1.2 Proposed project management techniques

7.1.3 Resources available to perform the work, including any specialized services, with the specified time limits for the project.

7.4.3.1 Technical Environment
7.4.3.2 Timeline

7.1.4 Cost

    7.4.4.1 Project cost
    7.4.4.2 Maintenance cost

7.1.5 Record of past performance including price and cost data from previous projects, quality of work, ability to meet schedules, cost control and contract administration.

7.1.6 Ability and proven history in handling special project constraints

7.1.7 Availability to the project locale

7.1.8 Familiarity with the project locale

SD DCI reserves the right to reject any or all proposals, waive technicalities, and make award(s) as deemed to be in the best interest of SD DCI.

7.2

Experience and reliability of the Offeror's organization are considered subjectively in the evaluation process. Therefore, the Offeror is advised to submit any information which documents successful and reliable experience in past performances, especially those performances related to the requirements of this RFP.

7.3

The qualifications of the personnel proposed by the Offeror to perform the requirements of this RFP, whether from the Offeror's organization or from a proposed subcontractor, will be subjectively evaluated. Therefore, the Offeror should submit detailed information related to the experience and qualifications, including education and training, of proposed personnel.

7.4 Award

The requesting agency and the highest ranked Offeror shall mutually discuss and refine the   scope of services for the project and shall negotiate contract terms, including compensation and performance schedule.

7.4.1 If the agency and the highest ranked Offeror are unable for any reason to negotiate a contract at a compensation level that is reasonable and fair to the agency, the agency shall, either orally or in writing, terminate negotiations with the vendor.   The agency may then negotiate with the next highest ranked vendor.

7.4.2 The negotiation process may continue through successive Offerors, according to agency ranking, until an agreement is reached, or the agency terminates the contracting process.

8.0 BEST AND FINAL OFFERS

SD DCI. DCI reserves the right to request best and final offers. If so, SD DCI will initiate the request for best and final offers; best and final offers may not be initiated by an Offeror.   Best and final offers may not be necessary if SD DCI is satisfied with proposals received.

If best and final offers are sought, SD DCI will document which Offerors will be notified and provide them opportunity to submit best and final offers. Requests for best and final offers will be sent stating any specific areas to be covered and the date and time in which the best and final offer must be returned. Conditions, terms, or price of the proposal may be altered or otherwise changed, provided the changes are within the scope of the request for proposals and instructions contained in the request for best and final offer. If an Offeror does not submit a best and final offer or a notice of withdrawal, the Offeror's previous proposal will be considered that Offeror's best and final proposal. After best and final offers are received, final evaluations will be conducted.

9.0 SCANNING

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

The Offeror should fill in the information below and sign the form. The Offeror's employee signing this form must have the authority to allow the State to do a security scan. If no security contact is given the State will assume that the State can scan at any time. **At the State's option, any RFP response that does not include a completed and signed form may be dropped from consideration. If there is State data protected by federal or state law or regulation or industry standard involved the State is more likely to consider a security scan necessary for an RFP to be considered.** The State will only provide scan information to the Offeror's security contact. At the State's option, the State will conduct the scan at a location named by the Offeror. The Offeror can only request, not require naming the scanning location. The State may consider a comprehensive, compete and recent risk assessment as satisfying the scanning requirement. If required, the State will sign a non-disclosure agreement before scanning or receiving the risk assessment. In the event scanning as contemplated in this Paragraph 9.0 is required to be completed prior to executing a contract under this RFP, the following form must be completed and signed by the Offeror.

Offeror's name: _____

Offeror's security contact's name: _____

Security contact's phone number: _____

Security contact's email address: _____

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

Offeror's employee acknowledging the right to scan (Print):

Title: _____

Date: _____

Signature: _____

APPENDIX B –Contract Terms and Conditions

STATE OF SOUTH DAKOTA
Consultant Contract
for Services
Between

State of South Dakota
Office of the Attorney General
1302 East Highway 14
Pierre SD 57501
(605)773-3215

Referred to as Vendor	¸Referred to as State̦

The State hereby enters into this agreement (the "Agreement" hereinafter) for services with the Vendor. While performing services hereunder, Vendor is an independent contractor and not an officer, agent, or employee of the State of South Dakota.

A.   STANDARD PROVISIONS

1.   VENDOR

The Vendor will provide the State with its Vendor Number, Employer Identification Number, Federal Tax Identification Number or Social Security Number upon execution of this Agreement.

2.   PERIOD OF PERFORMANCE OF THIS AGREEMENT

This agreement shall be effective on _____and will end on _____, unless sooner terminated pursuant to the terms hereof. The State in its sole discretion may renew the Agreement under the same terms and conditions for up to four (4) one year periods. Notice of intent to renew shall be given by the State to the Vendor in writing prior to a term's expiration as provided in the Agreement. If notice of intent to renew is given, the Agreement shall renew unless terminated by either party pursuant to the Termination Provision of the Agreement.

3.   NOTICE

Any notice or other communication required under this Agreement shall be in writing and sent to the address set forth above. Notices shall be given by and to _____ on behalf of the State, and by and to _____, on behalf of the Vendor, or such authorized designees as either party may from time to time designate in writing. Notices or communications to or between the parties shall be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination shall be sent by registered or certified mail, or, if personally delivered, when received by such party.

4.   PROVISIONS (add an addendum if needed; if an addendum is used it is incorporated herein)

The Purpose of this Consultant Contract is to:

The Vendor agrees to perform the following services (add an attachment if needed.):

1.   The Vendor will perform those activities described in the Scope of Work attached hereto as Attachment A and incorporated herein.

C.   The Vendor further agrees, represents, and warrants that:

The Vendor will not use state equipment, supplies or facilities.
D. Will the State pay Vendor expenses as a separate item?
YES (   )   NO (   )

If YES, expenses submitted will be reimbursed as identified in this Agreement.

E. The TOTAL CONTRACT AMOUNT will not exceed $_____.

5. BILLING AND PAYMENT

The State will make payment for services upon satisfactory completion of the services. Vendor agrees to submit an itemized invoice for services within thirty (30) days following the month in which services were provided. Vendor agrees to submit a final itemized invoice within thirty (30) days of the Agreement end date to receive payment for completed services. As used herein, the term "end date" shall include the completion of any services pursuant to the Agreement, any extension period, or early termination of the Agreement. If a final itemized invoice cannot be submitted in thirty (30) days, then a written request for extension of time and explanation must be provided to the State.

Payment will be made consistent with SDCL ch. 5-26, as such, payment will be made within forty-five (45) days of the receipt of an itemized invoice submitted by the Vendor with a signed state voucher. The Vendor acknowledges that it would be difficult or impracticable for the State to provide the notice of disagreement provided for by SDCL 5-26-5 within the ten days provided for by that section. Accordingly, Vendor hereby agrees that the State shall have thirty (30) days to provide the requisite notice of disagreement

6. OVERPAYMENT

All payments to the Vendor by the State are subject to site review and audit as prescribed and carried out by the State. Any overpayment of this Agreement shall be returned to the State within thirty (30) days after written notification to the Vendor

7. LICENSING AND STANDARD COMPLIANCE

The Vendor agrees to comply in full with all laws, regulations, ordinances, guidelines, permits, requirements and other standards applicable to providing services under this Agreement, promulgated by any federal, state, tribal, or local government, and will be solely responsible for obtaining current information regarding the foregoing.

8. LICENSE AGREEMENTS

Vendor warrants that, prior to the execution of this Agreement, it has provided to the State and incorporated into this agreement dated, physical copies of all license agreements, End User License Agreements, and terms of use regarding its software or any software incorporated into its software. Failure to provide all such license agreements, End User License Agreements, and terms of use shall be a breach of this agreement at the option of the State. The parties agree that neither the State nor its end users shall be bound by the terms of any such agreements not timely provided pursuant to this paragraph and incorporated into this Agreement. Vendor agrees that it shall indemnify and hold the State harmless from any and all damages or other detriment, actions, lawsuits or other proceedings that arise from failure to provide all such license agreements, End User License Agreements, and terms of use or that arise from any failure to give the State notice of all such license agreements, End User License Agreements, and terms of use. Any changes to the terms of the agreements described in this paragraph must first be agreed to by both parties in writing before they go into effect. This paragraph shall control and supersede the language of any such agreements to the contrary.

9. TERMINATION

This Agreement may be terminated by either party hereto upon thirty (30) days written notice. In the event the Vendor breaches any of the terms or conditions hereof, this Agreement may be terminated by the State for cause at any time, with or without notice. If termination for such a default is effected by the State, any payments due to Vendor at the time of termination may be adjusted to cover any additional costs to the State because of Vendor's default. Upon termination the State may take over the work and may award another party an agreement to complete the work under this Agreement. If after the State terminates for

a default by Vendor it is determined that Vendor was not at fault, then the Vendor shall be paid for eligible services rendered and expenses incurred up to the date of termination. Upon termination of this Agreement in all other circumstances, all accounts and payments shall be processed according to financial arrangements set forth herein for services rendered to date of termination.

Upon the effective date of the termination of the Agreement the Vendor will return all Confidential Information, state proprietary information, state data and end user data in a non-proprietary form.

In the event that the Vendor fails to complete the project or any phase thereof within the time specified in the Scope of Work, attached hereto as "Attachment A", or within such additional time as may be granted in writing by the State, or fails to perform the work, or any separable part thereof, with such diligence as will insure its completion within the time specified in the Scope of Work or any extensions thereof, the State shall be authorized to terminate the Agreement for default and suspend the payments scheduled as set forth elsewhere in this Agreement.

In the event this Agreement is to be terminated by the State pursuant to Paragraph 11 (FUNDING), the Agreement may be terminated by the State upon five (5) business days written notice.

10. SURVIVAL FOLLOWING TERMINATION

The confidentiality, indemnity and records retention provisions survive termination of the Agreement between the parties

11. FUNDING

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 the law or federal funds reduction, 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.

12. ASSIGNMENT AND AMENDMENT

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

13. CONTROLLING LAW

This Agreement shall be governed by and construed in accordance with the laws of the State of South Dakota, without regard to any conflicts of law principles, decisional law, or statutory provision which would require or permit the application of another jurisdiction's substantive law. Venue for any lawsuit pertaining to or affecting this Agreement shall be in the Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota.

14. SUPERCESSION

All 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.

15. SEVERABILITY

In the event that any provision of this Agreement shall be held unenforceable or invalid by any court of competent jurisdiction, such holding shall not invalidate or render unenforceable any other provision of this Agreement, which shall remain in full force and effect.

16. WORK PRODUCTS

Vendor hereby acknowledges and agrees that all reports, plans, specifications, technical data, drawings, software system

programs and documentation, procedures, files, operating instructions and procedures, source code(s) and documentation, including those necessary to upgrade and maintain the software program, state data, end user data, and all information contained therein provided to the State by the Vendor in connection with its performance of service under this Agreement, and any Confidential Information as defined in the Confidentiality of Information paragraph herein, shall belong to and is the property of the State and will not be used in any way by the Vendor without the written consent of the State.

Paper, reports, forms software programs, source code(s) and other materials which are a part of the work under this Agreement will not be copyrighted without written approval of the State. In the unlikely event that any copyright does not fully belong to the State, the State none the less reserves a royalty-free, non-exclusive, and irrevocable license to reproduce, publish, and otherwise use, and to authorize others to use, any such work for government purposes.

Vendor agrees to return all information received from the State to State's custody upon the end of the term of this Agreement, unless otherwise agreed in a writing signed by both parties.

17. THIRD PARTY BENEFICIARIES

This Agreement is intended only to govern the rights and interests of the parties named herein. It is not intended to, does not and may not be relied upon to create any rights, substantial or procedural, enforceable at law by any third party in any matters, civil or criminal.

18. SUBCONTRACTORS

The Vendor may not use subcontractors to perform the services described herein without express prior written consent from the State.

The Vendor 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 Vendor 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. The State, at its option, may require the vetting of any subcontractors. The Vendor is required to assist in this process as needed.

19. STATE'S RIGHT TO REJECT

The State reserves the right to reject any person from the Agreement who the State believes would be detrimental to the project, presents insufficient skills, presents inappropriate behavior or is considered by the State to be a security risk.

20. HOLD HARMLESS AND INDEMNIFICATION

The Vendor agrees to hold harmless and indemnify the State of South Dakota, its officers, agents and employees, from and against any and all actions, suits, damages, liability or other proceedings which may arise as the result of performing services hereunder, including reasonable attorney's fees. This section does not require the Vendor to be responsible for or defend against claims or damages arising solely from errors or omissions of the State, its officers, agents or employees. The foregoing indemnification language likewise applies to claims arising from or relating to a third party claim that any of the services or deliverables provided by Vendor to the State under this Agreement infringes that party's U.S. patent, U.S. trademark or copyright or misappropriates that party's trade secret or other intellectual property right; provided that Vendor, in this circumstance, shall not be required to indemnify State and its affiliates for any claims that result from or are related to: (i) the State's or other party's combination, operation, or use of the software in a manner not specifically authorized by Vendor; or (ii) alterations or modifications to the software not performed or authorized by Vendor.

21. INSURANCE

Before beginning work under this Agreement, Vendor shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement. The Vendor, at all times during the term of this Agreement, shall obtain and maintain in force insurance coverage of the types and with the limits listed below. In the event of a substantial change in insurance, issuance of a new policy, cancellation or nonrenewal of a policy, the Vendor agrees to provide immediate notice to the State and provide a new certificate of insurance showing continuous coverage in the amounts required. Vendor shall furnish copies of insurance policies if requested by the State.

A. Commercial General Liability Insurance:
Vendor shall maintain occurrence-based commercial general liability insurance or an 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.

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

C. Worker's Compensation Insurance:
Vendor shall procure and maintain Workers' Compensation and employers' liability insurance as required by South Dakota law.

22. CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY, AND VOLUNTARY EXCLUSION

By signing this Agreement, Vendor certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by the federal government or any state or local government department or agency. Vendor further agrees that it will immediately notify the State if during the term of this Agreement either it 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.

23. BACKGROUND CHECKS

The State of South Dakota requires all employee(s) of the vendor, subcontractors, agents, assigns and or affiliated entities who write or modify State of South Dakota-owned software, alter hardware, configure software of state-owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas, to undergo fingerprint-based background checks. These fingerprints will be used to check the criminal history records of the State as well as the Federal Bureau of Investigation's criminal history records. These background checks must be performed by the State with support from the State's law enforcement resources. The State will supply the finger print cards and prescribe the procedure to be used to process the finger print cards. Project plans should allow two (2) to four (4) weeks to complete this process. If work assignments change after the initiation of the project covered by this agreement so that employee(s) of the vendor, subcontractor's, agents, assigns and or affiliated entities will be writing or modifying State of South Dakota owned software, altering hardware, configuring software of state owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas then, background checks must be performed on any employees who will complete any of the referenced tasks. The State reserves the right to require the Vendor to prohibit any employee, subcontractors, agents, assigns and or affiliated entities from performing work under this Agreement whenever the State, in its sole discretion, believes that having a specific employee, subcontractor, agent assign or affiliated entity 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 check. The State will provide the Vendor with notice of this determination.

24. RECORDS RETENTION

The Vendor will comply with any applicable records retention provisions under State and/or federal law. Further, it is the responsibility of the Vendor to identify any and all such provisions regarding record retention.

25. REPORTING PROVISION

Vendor agrees to report to the State any event encountered in the course of performance of this Agreement which results in injury to any person or property, or which may otherwise subject Vendor, or the State of South Dakota or its officers, agents or employees to liability. Vendor shall report any such event to the State immediately upon discovery.

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

26. CONFIDENTALITY OF INFORMATION

For the purpose of this Agreement, "Confidential Information" shall include all information disclosed to the Vendor by the State and all information obtained by the Vendor through the provisions of services as contemplated by this Agreement. The Vendor, and any person or entity affiliated with the Vendor shall not disclose any Confidential 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, and any person or entity affiliated with the Vendor shall not: (i) disclose any Confidential Information to any third person unless otherwise specifically allowed under this Agreement; (ii) make any use of Confidential Information except to exercise rights and perform obligations under this Agreement; (iii) make Confidential Information available to any of its employees, officers, agents or consultants except those who have agreed to obligations of confidentiality at least as strict as those set out in this Agreement and who have a need to know such information. The Vendor, and any person or entity affiliated with the Vendor is held to the same standard of care in guarding Confidential Information as it applies to its own confidential or proprietary information and materials of a similar nature, and no less than holding Confidential Information in the strictest confidence. The Vendor, and any person or entity affiliated with the Vendor shall protect 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. Confidential Information shall not include information that:
1.   was in the public domain at the time it was disclosed to the Vendor, or any person or entity affiliated with the Vendor;
2.   was known to the Vendor, or any person or entity affiliated with the Vendor without restriction at the time of disclosure from the State;
3.   that was disclosed with the prior written approval of State's officers or employees having authority to disclose such information;
4.   was independently developed by the Vendor, or any person or entity affiliated with the Vendor without the benefit or influence of the State's information;
5.   becomes known to the Vendor, or any person or entity affiliated with the Vendor, without restriction, from a source not connected to the State of South Dakota.

 Confidential Information can include names, social security numbers, employer numbers, addresses and all other data about applicants, participants, employers or other clients to whom the State provides services of any kind. Vendor understands that this information may be confidential and protected under applicable State law at SDCL 1-27-1.5, modified by SDCL 1-27-1.6. Vendor agrees to immediately notify the State if the information is disclosure, either intentionally or inadvertently. The parties mutually agree that neither of them shall disclose the contents of the 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. Vendor acknowledges that the State and its agencies are public entities and thus are 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 the South Dakota open records or open meetings laws.   If work assignments performed in the course of this Agreement require additional security requirements or clearance, the Vendor agrees that its officers, agents and employees may be required to undergo investigation or may be required to sign separate confidentiality agreements, and it will limit access to the confidential information and related work activities to employees that have executed such agreements.

The Vendor will enforce the terms of this Confidentiality Provision to its fullest extent. The Vendor agrees to remove any employee or agent from performing work under this Agreement that has or is suspected to have violated the terms of this Confidentiality Provision and to immediately notify the State of such matter.

The Vendor will require every person or entity however affiliated with the Vendor who will have access to Confidential Information to be under a contractual obligation of nondisclosure at least as stringent as that required by this Agreement; and will limit access

to any Confidential Information to those persons or entities who have a need to know and who have been instructed that such information is confidential under state law.

The Vendor will comply with any other confidentiality measures and terms included in the Agreement.

Upon termination of this Agreement, if not already done so as part of the services performed under the Agreement, the Vendor agrees to return to the State, at the Vendor's cost, any Confidential Information or documentation maintained by the Vendor regarding the services provided hereunder in a format readily useable by the State as mutually agreed by the Vendor and State.

27. FORCE MAJEURE

Notwithstanding anything in this Agreement to the contrary, neither party shall be liable for any delay or failure to perform under the terms and conditions of this Agreement, if the delay or failure is caused by war, terrorist attacks, riots, civil commotion, fire, flood, earthquake or any act of God, or other causes beyond the party's reasonable control. Provided, however, that in order to be excused from delay or failure to perform, the party must act diligently to remedy the cause of such delay or failure and must give notice to the other party as provided in this Agreement as soon as reasonably possible of the length and cause of the delay in performance.

28. DILIGENCE AND SKILL

A. In the performance of these services and providing the deliverables under the Agreement, Vendor, and its employees shall exercise the degree of skill and care consistent with customarily accepted practices and procedures for the performance of the type of services required. The Vendor shall be responsible for the professional quality, technical accuracy, timely completion, and coordination of all services and deliverables furnished by the Vendor and any subcontractors, if applicable, under this Agreement.

B. Vendor represents and warrants that:

   i. It shall give high priority to the performance of the services; and

   ii. The services shall be performed in a timely manner.

C. It shall be the duty of the Vendor to assure that its services and deliverables are technically sound and in conformance with all pertinent technical codes and standards.

D. The Vendor shall be responsible to the State for material deficiencies in the contracted deliverables and services which result from the failure to meet the standard given herein. Vendor shall promptly correct or revise any material errors or omissions in deliverables and re-perform any services which are not in compliance with such representations and warranties at no cost to the State, provided that Vendor's failure to comply is not related or attributable, in whole or in part, to the actions, errors or omissions of the State.

E. Permitted or required approval by the State of any services or deliverables furnished by the Vendor shall not in any way relieve the Vendor of its responsibility for the professional quality and technical accuracy and adequacy of its work. The State's review, approval, acceptance, or payment for any of the Vendor's services or deliverables herein shall not be construed to operate as a waiver of any rights under this Agreement or of any cause of action arising out of the performance of this Agreement, and except as provided herein the Vendor shall be and remain liable in accordance with the terms of this Agreement and applicable law for all damages to the State caused by the Vendor's performance or failure to perform under this Agreement.

F. In the event of a breach of these representations and warranties, the State shall provide telephonic notice to the Vendor. The State may, in its sole discretion, require Vendor to cure such breaches. If it is necessary for Vendor to send at least one qualified and knowledgeable representative to the State's site where the system is located, this will be done at Vendor's sole expense. This representative will continue to address and work to remedy the deficiency, failure, malfunction, defect, or problem at the site. The rights and remedies provided in this paragraph are in addition to any other rights or remedies provided in this Agreement or by law.

29. INTELLECTUAL PROPERTY

In connection with the performance of this Agreement and the provision of services and deliverables under this Agreement, neither party will infringe any patent, copyright, trademark, trade secret or other proprietary right of any person. Neither party will improperly use any trade secrets or confidential or proprietary information owned by any third party in performing this Agreement or the services related to this Agreement.

30. THIRD PARTY RIGHTS

The Vendor represents and warrants that it has the full power and authority to grant the rights described in this Agreement without violating any rights of any third party, and that there is currently no actual or, to Vendor's knowledge, threatened suit by any such third party based on an alleged violation of such rights by Vendor. The Vendor further represents and warrants that the person executing this Agreement for Vendor has actual authority to bind Vendor to each and every term, condition and obligation to this Agreement, and that all requirements of Vendor have been fulfilled to provide such actual authority.

31. COMPLIANCE WITH EXECUTIVE ORDER 2020-01:

Pursuant to Executive Order 2020-01, for contractors, vendors, suppliers, or subcontractors with five (5) or more employees who enter into a contract with the State of South Dakota that involves the expenditure of one hundred thousand dollars (100,000.00) or more, by signing this Agreement Contractor certifies and agrees that it 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 this Agreement, with a person or entity that is either the State of Israel, or a company doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel to do business, or doing business in the State of Israel, with the specific intent to accomplish a boycott or divestment of Israel in a discriminatory manner. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to terminate this Agreement. Contractor further agrees to provide immediate written notice to the State if during the term of this Agreement it no longer complies with this certification and agrees such noncompliance may be grounds for termination of this Agreement.

B. **BUREAU OF INFORMATION AND TELECOMMUNICATIONS (BIT CLAUSES)**

Pursuant to South Dakota Codified Law 1-33-44, the Bureau of Information and Telecommunications ("BIT" hereinafter) 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. BIT requires the contract provisions which are set forth this Section B (BIT CLAUSES) of this Agreement.   It is understood and agreed to by all parties that BIT has reviewed only Section B of this Agreement.

1. SECURITY

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

By signing this agreement, the Consultant warrants that:
  A. All Critical, High, Medium, and Low security issues are resolved. Critical, High and Medium can be described as follows:
      a. **Critical** - Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices.
      b. **High** - The vulnerability is difficult to exploit; however, it is possible for an expert in Information Technology. Exploitation could result in elevated privileges.
      c. **Medium** - Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. Denial of service vulnerabilities that are difficult to set up.
      d. **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 Consultant in performing an investigation to determine the nature of any security issues that are discovered or are reasonably suspected after acceptance. The Consultant 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.   The Consultant will fully support and maintain the Consultant'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 Consultant may not withhold support from the State for this application nor charge the State additional fees as a result of the State moving the Consultant's application to a new release of third-party technology if:
i.   The previous version of the third-party code base or platform is no longer being maintained, patched, and supported; and
ii.   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 Consultant may limit their support and maintenance to any one or all of the applicable third-party code bases or platforms.

If a code base or platform on which the Consultant's application depends is no longer supported, maintained, or patched by a qualified third party the Consultant commits to migrate its application from that code base and/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 Consultant to work in good faith with the State to secure or a timely move to supported, maintained, and patched technology will allow the State to cancel this Agreement without penalty.

2.   LICENSE TO PERFORM SECURITY SCANNING

The Consultant will provide the State, at a time and for duration agreeable to both parties, access to the application and underlying hardware referenced in this Agreement for security scanning activities. Any scanning performed by the State will not be considered a violation of any licensure agreements the State has with the Consultant or the Consultant has with a third-party. Scanning by the State or any third-party acting for the State will not be considered reverse engineering. If the state security scanning efforts discover security issues, the State may collaborate, at the State's discretion, with the Consultant on remediation efforts. These remediation efforts will not be considered a violation of any licensure agreements the State has with the Consultant. The State will be indemnified and held harmless by the Consultant from all actions, lawsuits, damages (including all ordinary, incidental, consequential, and exemplary damages) or other proceedings that arise from security scanning, remediation efforts, and any after effects of security scanning or remediation. This indemnification includes all defense costs as well as reasonable attorneys' fees the State of South Dakota is required to pay in any such proceedings. The State will not be charged for any costs incurred by Consultant in these remediation efforts unless agreed to by the State in advance in writing. In the event of conflicting language this clause supersedes any other language in this or any other agreement made between the State and the Consultant.

3.   THREAT NOTIFICATION

Upon becoming aware of a possible credible security threat with the Consultant's product(s) and or service(s) being used by the State, the Consultant or any subcontractor suppling product(s) or service(s) to the Consultant needed to fulfill the terms of this Agreement will notify the State within two (2) business days of any such threat. If the State requests, the Consultant will provide the State with information on the threat. A credible threat consists of the discovery of an exploit that a person considered an expert on Information Technology security believes could be used to breach one or more aspects of a system that is holding State data,   or   a   product   provided   by   the   Consultant.

4.   OFFSHORE SERVICES

The Consultant 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 or without the written permission of the State.

5.   USE OF ABSTRACTION TECHNOLOGIES:

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

The Vendor warrants that hard-coded references will not be used in the application. Use of hard-coded references will result in a

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

6. SECURITY INCIDENT NOTIFICATION:

a. 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 Vendor, unless stipulated otherwise, shall notify the State Contact within 24 hours if the Vendor reasonably believes there has been a security incident.

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 twelve (12) hours after law-enforcement provides permission for the release of information on the security incident or data breach.

b. Notification to the State should include at a minimum all data available including: (i) Name of and contact information for the Vendor's Point of Contact for the security incident or data breach: (ii) date and time of the security incident or data breach; (iii) date and time the security incident or data breach was discovered: (iv) description of the security incident or data breach including the data involved, being as specific as possible; (v) potential number of records known, and if unknown the range of records; (vi) address where the security incident or data breach occurred: and, (vii) the nature of the technologies involved. If not all of the information is available for the notification within the specified time period Vendor shall provide the State with all of the available information.

7. BROWSER:

The system, site, and/or application must be compatible with supported versions of Edge, Chrome, Safari, and Firefox browsers. QuickTime, PHP, Adobe ColdFusion, Adobe Flash and Adobe Animate CC will not be used in the system, site, and/or application.

8. SECURE PRODUCT DEVELOPMENT

By signing this agreement, the Consultant 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 Consultant'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 Consultant upon the Consultant signing a non-disclosure agreement.

9. MALICIOUS CODE

A. The Consultant warrants that the service contains no code that does not support an application requirement.
B. The Consultant warrants that the service contains no malicious code.
C. The Consultant warrants that the Consultant will not insert into the service or any media on which the software is delivered any malicious or intentionally destructive code.
D. The Consultant warrants that the Consultant will use commercially reasonable efforts consistent with industry standards to scan for and remove any malicious code from the licensed software before installation. In the event any malicious code is discovered in the licensed software delivered by the Consultant, the Consultant shall provide the State at no charge with a

copy of the applicable licensed software that contains no malicious code or otherwise correct the affected portion of the services provided to the State. The remedies in this paragraph are in addition to other additional remedies available to the State.

11. SOURCE CODE ESCROW

A. Deposit in Escrow: "Source Code" means all source code of the Software, together with all commentary and other materials supporting, incorporated into or necessary for the use of such source code, including all supporting configuration, documentation, and other resource files and identification by Consultant and version number of any software (but not a license to such third-party software) used in connection with the source code and of any compiler, assembler, or utility used in generating object code.

1. Within ninety (90) days of the effective date, Consultant shall deposit the Source Code for the software with a nationally recognized software escrow company (subject to the approval of the State, not to be unreasonably withheld) (the "Escrow Agreement"). Within thirty (30) days after delivery to Customer of any major update, Consultant shall deposit the Source Code for such update with the Escrow Agent pursuant to the Escrow Agreement. For all other updates, Consultant shall deposit the Source Code for such updates on a semiannual basis with the Escrow Agent pursuant to the Escrow Agreement.

2. The parties agree that the Escrow Agreement is an "agreement supplementary to" the Agreement as provided in Section 365(d) of Title 11, United States Code (the "Bankruptcy Code"). Immediately upon termination of this Agreement, the Source Code shall be released back to Consultant.

B. Conditions for release: The State will have the right to obtain the Source Code in accordance with and subject to the terms and conditions of this Section and the Escrow Agreement provided that all of the following three conditions are met (collectively a "Release Event"):

1. Consultant winds down its business or liquidates its business under a Chapter 7 Bankruptcy proceeding; or Consultant discontinues maintenance and support to the Software,

2. No entity has succeeded to Consultant's obligations to provide maintenance and support on the Software in accordance with the Agreement in effect between the parties, and

3. The State is not in breach of its obligations under this Agreement.

C. Source Code: In no event shall the State have the right to use the Source Code "barring a release event" for any purpose, and the State is specifically prohibited from using the Source Code to reverse engineer, develop derivative works or to sublicense the right to use the Source Code to any other person or entity for any purpose. Customer will also be obligated to treat the Source Code as Confidential Information of Consultant under the Agreement.

The cost for establishing and maintaining the Escrow Account will be that of the State.

12. DENIAL OF ACCESS OR REMOVAL OF AN APPLICATION AND OR HARDWARE FROM PRODUCTION

During the life of this Agreement the application and or hardware can be denied access to or removed from production at the State's discretion. The reasons for the denial of access or removal of the application and or hardware from the production system may include but not be limited to security, functionality, unsupported third-party technologies, or excessive resource consumption. Denial of access or removal of an application and or hardware also may be done if scanning shows that any updating or patching of the software and or hardware produces what the state determines are unacceptable results. The Consultant will be liable for additional work required to rectify issues concerning security, functionality, unsupported third-party technologies, and or excessive consumption of resources if it is for reasons of correcting security deficiencies or meeting the functional requirements originally agreed to for the application and or hardware. At the discretion of the State, contractual payments may be suspended while the application and or hardware is denied access to or removed from production. The reasons can be because of the Consultant's actions or inactions. Access to the production system to perform any remedying of the reasons for denial of access or removal of the software and hardware, and its updating and or patching will be made only with the State's prior approval. It is expected that the

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

13.   MOVEMENT OF PRODUCT

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

14.   USE OF PRODUCT ON VIRTUALIZED INFRASTRUCTURE AND CHANGES TO THAT INFRASTRUCTURE

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

15.   LOAD BALANCING

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

16.   BACKUP COPIES

The State may make and keep backup copies of the licensed product without additional cost or obligation on the condition that:
    A.   The State maintains possession of the backup copies.
    B.   The backup copies are used only as bona fide backups.

17.   SECURITY SCANNING

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

At the State's discretion, security scanning will be performed and or security settings put in place or altered during the software development phase and during pre-production review for new or updated code. These scans and tests, initially applied to development and test environments, can be time consuming and should be accounted for in project planning documents and

schedules. Products not meeting the State's security and performance requirements will not be allowed into production and will be barred from User Acceptance Testing (UAT) until all issues are addressed to the State's satisfaction. The discovery of security issues during UAT are automatically sufficient grounds for non-acceptance of a product even though a product may satisfy all other acceptance criteria. Any security issues discovered during UAT that require product changes will not be considered a project change chargeable to the State. The State urges the use of industry scanning/testing tools and recommends secure development methods are employed to avoid unexpected costs and project delays. Costs to produce and deliver secure and reliable applications are the responsibility of the Consultant 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.

18. PROVISION OF DATA

Upon notice of termination by either party, the State will be provided by the Consultant all current State Data and End User Data in a non-proprietary form. Upon the effective date of the termination of the agreement, the State will again be provided by the Consultant with all current State Data and End User Data in a non-proprietary form.

C.   AUTHORIZED SIGNATURES:

In Witness Whereof, the parties signify their agreement effective the date below first written by the signatures affixed below. By signing this agreement, the Bureau of Information and Telecommunications (BIT) is representing that as the State's technology governing organization it has reviewed only the technical provisions of this agreement

State   **Vendor**

_____   _____

(Signature)   (Signature)

BY: JASON RAVNSBORG   BY:_____
       ATTORNEY GENERAL   (Name)
       SOUTH DAKOTA OFFICE
       OF THE ATTORNEY GENERAL   _____

                                                                                              (Title)

DATE:_____   _____

                                                                                              (Vendor)

                                                                                              _____

                                                                                              (Date)

BY:_____
       Jeff Clines (As to Section B only)
       Commissioner, Bureau of Information
       And Telecommunications

DATE: _____

-Name and phone number of contact person in State Agency who can provide additional information regarding this contract, please contact Kelsey Roth at 605-773-3215.
-This contract will be paid out of the following funds: _____

EXHIBIT A
WORK PLAN

Appendix (Attachment) C
Security and Contractor Questions

Agencies: The following questions facilitate agencies acquiring technology that meets state security standards. These questions will assist in improving the quality and the timeliness of the procurement. BIT recommends that you utilize your BIT Point of Contact 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.

If you do not know the details of the technologies that vendors 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).

Contractors: The following questions help the state determine the best way to assess and integrate your product or service technology with the state's technology infrastructure. Some questions may not apply to the technology you use. In such cases, simply mark the question as NA (Not Applicable). You will see that these questions are divided into sections to help identify the point of the questions.
Use the last column as needed to explain your answers. Also note that 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 greyed out. **If the contractor answers a question by referencing another document or another part of the RFP response, they must give the page number and paragraph where the information can be found.**

The "BIT" column corresponds to the branch that will be the primary reviewers. If you have questions about the meaning or intent of a question, we can contact them on your behalf. DDC = Data Center; DEV = Development; TEL = Telecommunications; POC = Project Management office

Section A: System Security						
The following questions are relevant for all contractors 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	If there is a website that is used by State employees or the public as part of the offeror's solution the website must use SAML or OAUTH2 to provide single-sign-on.				
A2	DC TEL x	Will the system provide Internet security functionality on public portals using encrypted network/secure socket layer connections in line with current recommendations of the Open Web Application Security Project (OWASP)?				
A3	POC	Will the system have role-based access?				

#	BIT	Question	YES	NO	NA	Explain answer as needed
		Response				
A4	DC TEL	Does the application contain mitigations for risks associated to uncontrolled login attempts (response latency, re-Captcha, lockout, IP filtering, Multi Factor authentication)? Which mitigations are in place? What are the optional mitigations?				
A5	DC TEL	Are account credentials hashed and encrypted when stored?				
A6	DC TEL x	The protection of the State's system and data is of upmost importance. Security scans must be done if: • An application will be placed on the State's system. • The State's system connects to another system. • The contractor hosts State data. • The contractor has another party host State data the State will want to scan that party. **The State would want to scan a test system; not a production system and will not do penetration testing.** The scanning will be done with industry standard tools. Scanning would also take place annually as well as when there are code changes. Are either of these an issue? If so, please explain.				
A7	DC	Will SSL traffic be decrypted and inspected before it is allowed into your system?				
A8	POC x	Will organizations other than the State of South Dakota have access to our data?				
A9	DEV TEL	Do you have developers that possess software security related certifications (e.g., the SANS secure coding certifications)?				
A10	DEV	Are there some requirements for security that are "structured" as part of general release readiness of a product, and others that are "as needed" or "custom" for a particular release?				
A11	TEL	What threat assumptions were made, if any, when designing protections for the software and information assets processed?				
A12	TEL	How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used?				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
A13	TEL	What security criteria, if any, are considered when selecting third-party suppliers?				
A14	TEL	How has the software been measured/assessed for its resistance to publicly known vulnerabilities and/or attack patterns identified in the Common Vulnerabilities & Exposures (CVE®) or Common Weakness Enumerations (CWEs)? How have the findings been mitigated?				
A15	TEL	Has the software been evaluated against the Common Criteria, FIPS 140-2, or other formal evaluation process? If so, please describe what evaluation assurance level (EAL) was achieved, what protection profile the product claims conformance to, and indicate if the security target and evaluation report are available.				
A16	DC TEL	Are static or dynamic software security analysis tools used to identify weaknesses in the software that can lead to exploitable vulnerabilities? If yes, which tools are used? What classes of weaknesses are covered? When in the SDLC are these scans performed? Are SwA experts involved in the analysis of the scan results?				
A17	DC TEL x	Has the product undergone any vulnerability and/or penetration testing? If yes, how frequency, 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?				
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.				

#	BIT	Question	YES	NO	NA	Explain answer as needed
			Response			
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/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)?				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
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 done annually?				
		c. If it is SOC 2 audit report does it cover all 5 of the trust principles?				
		d. If it is a SOC 2 audit report what level is it?				
		e. Does the audit include cloud service providers?				
		f. Has the auditor always been able to attest to an acceptable audit result?				
		g. Will you provide a copy of your latest SOC 2 or ISO 27001 audit report upon request, a redacted version is acceptable?				
A36		Do you or your cloud service provider have any other security certification beside SOC 2 or ISO 27001, for example, FedRAMP or ITTRUST?				
A37	DC TEL	Are you providing a device or software that can be defined as being Internet of Thing (IoT)? Examples include IP camera, network printer, or connected medical device. If yes, what is your process for ensuring the software on your IoT devices that are connected to the state's system, either permanently or intermittently, are maintained and/or updated?				
A38	DC	Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all				

		registry settings?				

		Response				
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
A39	DC	What are your policies and procedures for hardening servers?				
A40	DC, TEL	(Only to be used when medical devices are being acquired.) Please give the history of cybersecurity advisories issued by you for your medical devices. Include the device, date and the nature of the cybersecurity advisory.				
A41	DC POC	Does any product you propose to use or provide the State include software, hardware or hardware components manufactured by any company on the US Commerce Department's Entity List?				
A42	DC	Describe your process for monitoring the security of your suppliers.				

Section B: Hosting
Only for Contractor hosted applications, systems, databases, services and any other technology not hosted on the State's infrastructure. Mark the questions as "NA" if this is an application hosted by the State.

#	BIT	Question	YES	NO	NA	Explain answer as needed
		Response				
B1	POC	Typically, the State of South Dakota prefers to host all systems. In if the State decides that it would be preferable for the vendor to host the system, is this an option?				
B2	POC	Are there expected periods of time where the application will be unavailable for use?				
B3	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?				
B4	DC	What are the procedures and policies used to control access to your servers? How are audit logs maintained?				
B5	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?				
B6	DC	Explain your tenant architecture and how tenant data is kept separately?				
B7	DC	What are your data backup policies and procedures? How frequently are your backup procedures verified?				
B8	DC DEV TEL	If any cloud services are provided by a third-party, do you have contractual requirements with them dealing with: · Security for their I/T systems; · Staff vetting; · Staff security training?				
		a. If yes, summarize the contractual requirements.				
		b. If yes, how do you evaluate the third-party's adherence to the contractual requirements?				
B9	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?				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
B10	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?				
B11	DC	How do you secure Internet of Things (IoT) devices on your network?				
B12	DC TEL	Do you use Content Threat Removal to extract and transform data?				
B13	DC TEL	Does your company have an endpoint detection and response policy?				
B14	DC TEL	Does your company have any real-time security auditing processes?				
B15	TELE	How do you perform analysis against the network traffic being transmitted or received by your application, systems and/or data center? What benchmarks do you maintain and monitor your systems against for network usage and performance? What process(es) and/or product(s) do you use to complete this analysis, and what results or process(es) can you share?				
B16	TELE	How do you monitor your application, systems and/or 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?				
B17	DC TELE	What anti-malware product(s) do you use?				
B18	DC TELE	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?				
B19	DC TELE	Have you ever had a data breach? If so, provide information on the breach.				
B20	POC	Is there a strategy for mitigating unplanned disruptions and what is it?				
B21	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?				
B22	POC	Will the State of South Dakota own the data created in your hosting environment?				
B23	DEV	What are your record destruction scheduling capabilities?				

Section C: Database

Applies to any application or service that stores data, irrespective of the application being hosted by the state or the vendor.

#	BIT	Question	Response			Explanation
			YES	**NO**	**NA**	
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 contractors or third parties engaged in providing this hardware, application or service and pertain to business practices. If the application is hosted by the contractor or the contractor supplies cloud services those questions dealing with installation or support of applications on the State's system can be marked "NA".

#	BIT	Question	Response			Explain answer as needed
			YES	**NO**	**NA**	
D1	DC POC	Will the contractor 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?				

#	BIT	Question	Response YES	NO	NA	Explain answer as needed
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 in question?				
		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?				

		Response				
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
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?				

#	BIT	Question	Response			Explain answer as needed
			YES	NO	NA	
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	TEL DC DEV	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	DC 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?				

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
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 pertain to the tools and third-party components used to develop your application, irrespective of the application being hosted by the State or the vendor

#	BIT	Question	YES	NO	NA	Explain answer as needed
E1	DEV POC x	What are the development technologies used for this system? Please indicate version as appropriate				
		ASP.Net				
		VB.Net				
		C#.Net				
		.NET Framework				
		Java/JSP				
		MS SQL				
		Other				
E2	DC TEL	Is this a browser-based User Interface?				
E3	DEV POC	Will the system have any workflow requirements?				
E4	DC	Can the system be implemented via Citrix?				
E5	DC	Will the system print to a Citrix compatible networked printer?				
E6	TEL	If your application does not run under the latest Microsoft operating system, what is your process for updating the application?				
E7	DEV	Identify each of the Data, Business and Presentation layer technologies your product would use and provide a roadmap outlining how your release and or update roadmap aligns with the release and 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?				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
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 so, 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 applications?				
E20	DC	Explain how and where the software validates (e.g., filter with white listing) 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)?				

#	BIT	Question	YES	NO	NA	Explain answer as needed
		b. Is it designed to isolate and minimize the extent of damage possible by a successful attack?				
Response						
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
E22	TEL	Does the program use run-time infrastructure defenses (such as address space randomization, stack overflow protection, preventing execution from data memory, and taint checking)?				
E23	TEL	If your application will be running on a mobile device what is your process for making sure your application can run on the newest version of the mobile device's operating system?				
E24	DEV	Do you use open source software or libraries? If yes, do you check for vulnerabilities in your software or library that are listed in:				
		a. Common Vulnerabilities and Exposures (CVE) database?				
		b. Open Source Vulnerability Database (OSVDB)?				
		c. Open Web Application Security Project (OWASP) Top Ten?				

Section F: Infrastructure

This pertains 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 as "NA".

#	BIT	Question	Response			
			YES	NO	NA	Explain answer as needed
F1	TEL	Is there a workstation install requirement?				
F2	DC	Will the system infrastructure have a special backup requirement?				
F3	DC	Will the system infrastructure have any processes that require scheduling?				
F4	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?				
F5	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?				
F6	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?				
F7	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.				
F8	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.				
F9	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.				
F10	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.				

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
F11	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.				
F12	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.				
F13	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?				
F14	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.				
F15	POC x	List any hardware or software you propose to use that is not State standard, the standards can be found at http://bit.sd.gov/standards/.				
F16	DC	Will your application require a dedicated environment?				
F17	DEV POC	Will the system provide an archival solution? If not, is the State expected to develop a customized archival solution?				
F18	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.				

#	BIT	Question	YES	NO	NA	Explain answer as needed
		Response				
F19	DC	Can the system be integrated with our enterprise Active Directory to ensure access is controlled?				
F20	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?				
F21	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. Symantec End Point Protection				
F22	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?				
F23	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?				
F24	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?				
F25	DC TEL	What physical access do you require to work on hardware?				
F26	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

These questions relate 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 the questions can be marked "NA".

#	BIT	Question	YES	NO	NA	Explain answer as needed
			Response			
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).				

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
G12	DC	Will you provide on-site support 24x7 to resolve security incidents? If not, what are your responsibilities in a security incident?				
G13	DEV	What training programs, if any, are available or provided through the supplier for the software? Do you offer certification programs for software integrators? Do you offer training materials, books, computer-based training, online educational forums, or sponsor conferences related to the software?				
G14	DC TEL	Are help desk or support center personnel internal company resources or are these services outsourced to third parties? Where are these resources located?				
G15	DC	Are any of the services you plan to use located offshore (examples include data hosting, data processing, help desk and transcription services)?				
G16	DC	Is the controlling share (51%+) of your company owned by one or more non-U.S. entities?				
G17	DC	What are your customer confidentiality policies? How are they enforced?				
G18	DC POC 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?				