STATE OF SOUTH DAKOTA
DEPARTMENT OF SOCIAL SERVICES
700 GOVERNORS DRIVE
PIERRE, SD 57501

Check-In/Queueing and Client Information System

PROPOSALS ARE DUE NO LATER THAN APRIL 30, 2025 BY 5PM CST

RFP13685 State POC: Kirsten Blachford EMAIL: Kirsten.Blachford@state.sd.us

READ CAREFULLY

FIRM NAME: ______________________ AUTHORIZED SIGNATURE: ______________________
(Digital signature allowed)

ADDRESS: ______________________ TYPE OR PRINT NAME: ______________________

CITY/STATE: ______________________ TELEPHONE NO: ______________________

ZIP (9 DIGIT): ______________________ FAX NO: ______________________

E-MAIL: ____

PRIMARY CONTACT INFORMATION

CONTACT NAME: ______________________ TELEPHONE NO: ______________________

FAX NO: ______________________ E-MAIL: ______________________

1.0 GENERAL INFORMATION

1.1 PURPOSE OF REQUEST FOR PROPOSAL (RFP)

DSS is seeking a software solution that will aid our visitors in having a smoother, modern experience that reduces wait times, improves service, improves communication, improves availability, and through such measures, reduce stress during an already stressful time in their lives.

The South Dakota Department of Social Services (DSS) assists children, families, individuals, seniors, and people with disabilities through some of the most difficult times in their lives. DSS intends to pilot this software at our new One Stop location (opening in February 2025). This location will DSS services for all constituents of Sioux Falls and the surrounding areas from a single location and is expecting over 150 visitors per day. If successful, DSS will consider expanding the use of the proposed software solution to our presence in over 40 communities across South Dakota.

1.2 ISSUING OFFICE AND RFP REFERENCE NUMBER

The Office of the Secretary is the issuing office for this document and all subsequent addenda relating to it, on behalf of the State of South Dakota, Department of Social Services. The reference number for the transaction is RFP13685. This number must be referred to on all proposals, correspondence, and documentation relating to the RFP.

1.3 LETTER OF INTENT

All interested offerors are requested to submit a non-binding Letter of Intent to respond to this RFP. While preferred, a Letter of Intent is not mandatory to submit a proposal.

Be sure to reference the RFP number in your letter.

The Letter of Intent must be submitted to Kirsten Blachford via email at Kirsten.Blachford@state.sd.us no later than March 18, 2025**.** Please place the following in the subject line of your email: Letter of Intent for RFP13685.

1.4 SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)

RFP Publication	03/12/2025
Letter of Intent to Respond Due	03/18/2025
Offeror Questions Due	04/01/2025
Responses to Offeror Questions	04/15/2025
Request for SFTP folder	04/29/2025
Proposal Submission	04/30/2025
Oral Presentations/discussions (if required)	Week of May 12, 2025
Proposal Revisions (if required)	TDB
Technical Review	Week of May 26, 2025
Anticipated Award Decision/Contract Negotiation	06/10/2025

1.5 SUBMITTING YOUR PROPOSAL

All proposals must be completed and received in the Department of Social Services by the date and time indicated in the Schedule of Activities.

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

Proposals must be submitted as PDFs via Secured File Transfer Protocol (SFTP). Offerors must request an SFTP folder no later than the date indicated in the Schedule of Activities by emailing Kirsten Blachford at Kirsten.Blachford@state.sd.us.

The subject line should read RFP13685 SFTP Request. The email should contain the name and the email of the person who will be responsible for uploading the document(s).

Please note, offeror will need to work with their own technical support staff to set up an SFTP compatible software on offeror's end. While the State of South Dakota can answer questions, State of South Dakota is not responsible for the software required.

All proposals may be signed in ink or digitally by an officer of the offeror legally authorized to bind the offeror to the proposal and sealed in the form intended by the respondent. Proposals that are not properly signed may be rejected.

No proposal may be accepted from, or any 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.

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

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

1.7 NON-DISCRIMINATION STATEMENT

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

1.8 CERTIFICATION RELATING TO PROHIBITED ENTITY

For contractors, vendors, suppliers, or subcontractors who enter into a contract with the State of South Dakota by submitting a response to this solicitation or agreeing to contract with the State, the bidder or offeror certifies and agrees that the following information is correct:

> The bidder or offeror, in preparing its response or offer or in considering proposals submitted from qualified, potential vendors, suppliers, and subcontractors, or in the solicitation, selection, or commercial treatment of any vendor, supplier, or subcontractor, is not an entity, regardless of its principal place of business, that is ultimately owned or controlled, directly or indirectly, by a foreign national, a foreign parent entity, or foreign government from China, Iran, North Korea, Russia, Cuba, or Venezuela, as defined by SDCL 5-18A. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to reject the bid or response submitted by the bidder or offeror on this project and terminate any contract awarded based on the bid or response. The successful bidder or offeror further agrees to provide immediate written notice to the contracting executive branch agency if during the term of the contract it no longer complies with this certification and agrees such noncompliance may be grounds for contract termination.

1.9 RESTRICTION OF BOYCOTT OF ISRAEL

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

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

1.10 CERTIFICATION OF NO STATE LEGISLATOR INTEREST

Offeror (i) understands neither a state legislator nor a business in which a state legislator has an ownership interest may be directly or indirectly interested in any contract with the State that was authorized by any law passed during the term for which that legislator was elected, or within one year thereafter, and (ii) has read South Dakota Constitution Article 3, Section 12 and has had the opportunity to seek independent legal advice on the applicability of that provision to any Agreement entered into as a result of this RFP. By signing an Agreement pursuant to this RFP, Offeror hereby certifies that the Agreement is not made in violation of the South Dakota Constitution Article 3, Section 12.

1.11 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.

1.12 OFFEROR INQUIRIES

Offerors may email inquiries concerning this RFP to obtain clarification of requirements. No inquiries will be accepted after the date and time indicated in the Schedule of Activities. Inquiries must be emailed to Kirsten Blachford at Kirsten.Blachford@state.sd.us with the subject line RFP13685 Inquiries.

The State will to respond to offeror's inquiries (if required) via e-mail. In addition, all inquiries and the State's responses will be posted on the state's e-procurement system and the DSS website at http://dss.sd.gov/keyresources/rfp.aspx. Offerors 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. Offerors will be notified in the same manner as indicated above regarding any modifications to this RFP.

1.13 PROPRIETARY INFORMATION

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

1.14 LENGTH OF CONTRACT

The contract resulting from this RFP will be issued for the period of approximately one (1) year ending May 31, 2026, with the option for renewal for up to three (3), one (1) year contracts at the discretion of the State based on performance and/or the continued availability of funds. Contracts will be negotiated on an annual basis.

1.15 GOVERNING LAW

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

1.16 DISCUSSIONS WITH OFFERORS (ORAL PRESENTATION/NEGOTIATIONS)

An oral presentation by an offeror to clarify a proposal may be required at the sole discretion of the State. However, the State may award a contract based on the initial proposals received without discussion with the Offeror. If oral presentations are required, they will be scheduled after the submission of proposals. Oral presentations will be made at the offeror's expense.

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

2.0 STANDARD CONTRACT TERMS AND CONDITIONS

Any contract or agreement resulting from this RFP will include the State's standard terms and conditions as listed below and as seen in **Attachment A**, the State's standard Information Technology ("IT") contract terms listed in **Attachment B**, along with any additional terms and conditions that may be necessary to the performance of the scope of work. The offeror must indicate in its response any issues it has with specific IT contract terms. If the offeror does not indicate that there is an issue with a specific IT contract term, then the offeror will be deemed to have accepted the IT contract terms as written.

2.1 The Contractor will perform those services described in the Scope of Work, attached hereto as Section 3.0 of the RFP and by this reference incorporated herein.

2.2 The Contractor's services under this Agreement shall commence on and end on , unless sooner terminated pursuant to the terms hereof.

2.3 The Contractor will use State equipment, supplies or facilities. **YES (** **)** **NO (** X **)**

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

2.5 The State will make payment for services upon satisfactory completion of the services. The TOTAL CONTRACT AMOUNT is an amount not to exceed $. The State will not pay Contractor's expenses as a separate item. Payment will be made pursuant to itemized invoices submitted with a signed state voucher. Payment will be made consistent with SDCL ch. 5-26.

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

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

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

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

C. Business Automobile Liability Insurance:

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

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

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

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

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

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

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

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

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

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

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

2.15 The Contractor may not use subcontractors to perform the services described herein without the express prior written consent of the State. The Contractor will include provisions in its subcontracts requiring its subcontractors to comply with the applicable provisions of this Agreement, to indemnify the State, and to provide insurance coverage for the benefit of the State in a manner consistent with this Agreement. The Contractor will cause its subcontractors, agents, and employees to comply, with applicable federal, state and local laws, regulations, ordinances, guidelines, permits and requirements and will adopt such review and inspection procedures as are necessary to assure such compliance.

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

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

2.18 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 , on behalf of the Contractor, or such authorized designees as either party may from time to time designate in writing. Notices or communications to or between the parties shall be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination shall be sent by registered or certified mail, or, if personally delivered, when received by such party.

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

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

3.0 SCOPE OF WORK

The Division of Social Services is publishing this RFP to obtain a secure software solution that will aid various divisions of DSS in improving the customer experience for walk-in and appointment in-person constituents visiting DSS facilities.

The following sections describe the expectations for an offeror’s response and the work which needs to be conducted.

3.1 General Overview

3.1.1 A summary overview of your understanding of what needs to be done and your methodology for project management and expected timeline to implement the software. Include specialized expertise, capabilities, and technical competencies that will be leveraged during implementation and after.

3.1.2 Narrative describing similar implementations, including references for DSS to contact regarding said implementations, including price and cost data, quality of work, ability to meet schedules, cost control, contract administration, traffic volume, number of agents, and any special project constraints.

3.2 Security

3.2.1 Security standards met by the proposed software, including any relevant certificates of compliance, most recent and next testing/compliance review dates, and/or links. Required standards: SOC2 and HIPAA.

3.2.2 Single-sign-on, detailed in Section 3.9, must be supported.

3.2.3 Narrative on how the proposed software stores, encrypts, and protects data gathered.

3.3 Functional Requirements

The proposed software solution is desired to have the following functions. Describe how the proposed software solution meets these specific requirements and include graphics/screenshots as needed.

3.3.1 The proposed software solution must support: multiple locations (services/staff/groups specific to specific locations), multiple groups/sub-groups of staff (at least three levels) with separate services, and staff assigned to multiple services.

3.3.2 Customer Interface/Notifications

3.3.2.1 Walk-in customers should be able to register for queueing- and appointment customers should be able to check-in for appointments – for all DSS services configured in the software via a customizable interface available on a tablet or PC in the lobby of a location.

3.3.2.1.1 Registration should be complete with the minimum of a name field, entered prior to selecting services for a specific appointment. Registration is only for the specific appointment and should not require setting a password or additional gathering of information unless the specific service requires it.

3.3.2.1.2 The customer should be able to register for a single or multiple services during a single check-in/registration session.

3.3.2.1.3 Notifications via SMS should be delivered to the customer to confirm registration/check-in if the customer has entered an optional mobile phone number. The mobile phone number MUST be an optional field.

3.3.2.2 The check-in interface should be customizable to include DSS branding, DSS internal personnel/service groupings and sub-groupings to at least three sub-levels.

3.3.2.3 The check-in interface should have customizable fields (enumerate in detail how many/other information pertinent to customizable fields for the proposed software solution).

3.3.2.4 The check-in/registration interface should have the ability to capture a picture of the customer.

3.3.2.5 The check-in/registration interface should have the ability to scan a standard government ID and use the information to complete the pertinent fields. The scan of the ID should not be stored in the system.

3.3.2.6 The check-in interface should display a customizable message per service after check-in with instructions.

3.3.2.7 If a customer does not wish to use the tablet/pc for check-in (or if DSS has not deployed such a device) the receptionist should be able to use the proposed software solution to register the customer as a walk-in or check-in the customer for an appointment.

3.3.2.8 After check-in/registration, the customer's entry should be queued for the requested service(s).

3.3.2.8.1 There should be a queue for each walk-in service. If a customer is registered for multiple services, they should appear in only one queue. DSS should be able to define priorities for which queue takes precedence when a customer register for multiple walk-in services.

3.3.2.8.2 The queue should be able to be displayed on digital signage with limited customer information (first/last initial and service and expected wait time) and updated in real time as the queue is worked by DSS staff.

3.3.2.8.3 When a DSS staff member uses the proposed software solution to select a queued customer entry, the customer should receive a SMS message (customized per service) and digital signage should be able to display a message.

3.3.2.9 After service is complete, the proposed software solution should send a customizable SMS to the customer. Ideally this can include a link to a customer-satisfaction survey included as part of the proposed software solution.

3.3.3 Receptionist Capabilities

3.3.3.1 The receptionist should have a view of all waiting customers across all queues/services, including time since registration.

3.3.3.1.1 If a customer has been waiting beyond a configurable amount of time per service, some sort of indication/notification should be provided to the receptionist and any supervisory staff for the queue/service.

3.3.3.2 If a customer arrives for an appointment that is not scheduled via the proposed software solution, the receptionist should have a procedure to receive notification and use the proposed software solution to assign the customer to the appropriate DSS staff member, if the staff member is available.

3.3.3.2.1 The receptionist should be able to see if the DSS staff member is available. The DSS staff member should then receive notification.

3.3.3.3 The receptionist should be able to change the queue/service, add additional information (notes, flags or other indicators), of a customer's registration/entry manually as needed.

3.3.3.4 Receptionists should be able to see appointments made for groups or individuals using the proposed software solution.

3.3.3.5 Receptionists should be able to see previous visits/appointments and the notes related if allowed by permissions to those groups/services.

3.3.3.6 Ability to print badges as designated in item 3.3.5.2 of this scope of work from the receptionist desk.

3.3.4 Agent Capabilities

3.3.4.1 Notifications for walk-in customers and appointment customers should be delivered to the appropriate staff group/staff member when the customer registers/checks-in at a DSS facility.

3.3.4.2 Agents should be able to only see the queues to which they are assigned.

3.3.4.3 Agents must be able to receive notifications only when they are available for service. Logging in/out of the software/mobile app for notification does suffice for this.

3.3.4.4 Agents must receive notifications on mobile devices and desktop (optionally via email). Browser notifications will suffice for desktops. SMS or app notifications will suffice for mobile devices.

3.3.4.5 Mobile device notifications must occur when the device is locked.

3.3.4.6 Mobile device notifications must occur without having a specific website/app open and "active" on screen.

3.3.4.7 Agents should be able to select a "room/window" in which to serve a customer prior to calling the customer to service.

3.3.4.8 Agents should be able to indicate/record if a customer does not respond to a call to service.

3.3.4.9 Agents should be able to make notes, add custom tags/flags/indicators to a customer's entry during service.

3.3.4.10 Agents should be able to record the outcome of the service, preferably with a custom defined set of statuses that are available in reporting. Example: Customer did not respond, Service complete successfully, Customer was delayed in arrival, Customer needed a different service).

3.3.4.11 Agents should be able to route the customer's entry to another queue/service after completing. When routed in such a manner, the customer's wait time during this visit should be considered and queued accordingly for the newly assigned queue/service.

3.3.4.12 Agents should be able to put a service on hold and call another customer. Example: A customer needed their ID but left it in the car. The agent puts the customer's service in some form of "on hold" and calls another customer. Once complete, the agent can then "resume" the previous customer's service and call them back for service again. Recording time to completion of service should accurately reflect the pause of service in such a situation.

3.3.4.13 Agents should be able to see previous visits/appointments and the notes related if allowed by permissions to those groups/services.

3.3.5 General Functions

3.3.5.1 The proposed software solution should support multiple languages on all interfaces and notifications.

3.3.5.2 SMS sending/receiving must be handled by the proposed software solution and not require DSS to acquire a third-party solution that is billed separately from this RFP.

3.3.5.3 Availability to print visitor “badges” in some form (i.e. sticker, etc.) either at the kiosk or at the receptionist desk. This must be customizable and configurable per service and have customizable badges per service. The badge should have some unique identifier on each badge printed.

3.4 Reporting Requirements

The proposed software solution must have robust data collection and reporting. Give examples of pertinent reports and include graphics/screenshots as needed. At minimum, DSS is requiring the following reports:

3.4.1 Average time to completion for a service, available by location, group, agent, day of week, month of year, hours/days.

3.4.2 Average wait time for a service, available by location, group, agent, day of week, month of year, hours/days.

3.4.3 Ideally, the proposed software solution can include customer-satisfaction survey results, available by location, group, agent, day of week, month of year, hours/days.

3.4.4 Availability of a report that details time-in/time-out of all badged visitors for a specific service or set of services that can output in a printable format as well as Excel/CSV for a specified timeframe.

3.5 Appointment Requirements

The proposed software solution should have the capability to allow customers to schedule appointments via an online app.

3.5.1 Appointments should synchronize and use availability from agent’s Microsoft 365 Outlook calendar.

3.5.2 If the proposed software solution requires an account be created in the online app (mobile or-web-based), the login must be integrated with mySD, the State’s citizen portal for single-sign on.

3.5.3 Appointments should be able to be scheduled only for a configurable time into the future (example: 1 week).

3.5.4 Appointments should be able to be scheduled with a group or an individual, based on the service configuration by DSS.

3.5.5 Availability of appointments should be customizable by group(s) and service(s) combination.

3.5.6 Availability to have appointments involve more than one agent/staff member, either manually on the employee interface or available as a configuration per service for the customer facing interface.

3.5.7 Availability to have appointments with multiple customers, either manually on the employee interface or available as a configuration per service for the customer facing interface.

3.5.8 Availability of appointments with individual DSS staff members should be configurable to only be available in the proposed software solution for specific days/times and also take into account the pre-existing entries at time of reservation in a staff members Outlook365 calendar and ensure that customers cannot book individual appointments during such blocked-out days/times or during pre-existing appointments.

3.5.9 Appointments made for an individual should be included in the proposed software solution's calendar view.

3.5.10 Agents with an appointment scheduled with them individually via the proposed software solution should receive notifications via email, browser notification, or app notification of the approaching appointment at configurable intervals and also when the customer arrives and checks-in for the appointment.

3.5.11 Receptionists should be able to make appointments (with the same restrictions as customers making appointments) on behalf of a customer.

3.6 Training

Provide a narrative containing information on your training staff and their credentials, the methods of training you have used in the past, and the proposed plan methodology and timeline for training for this implementation. The requirements below must be included.

3.6.1 **Provide Training Materials:** Training Materials in the form of videos, topic specific articles, and other forms must be provided at minimum a month prior to Go Live. These materials must include some type of framework for DSS staff that have not been exposed to the proposed software solution to be able to self-train (i.e. a course/model). Examples: your training courses/models come in SCORM (or other industry standard) format that can imported into many Learning Management Systems; your training courses/models are available online for DSS staff and the main course syllabus or outline can be customized for DSS specific needs and systems.

3.6.2 **Train the trainer:** Provide live training sessions for DSS staff that will become the trainers for the proposed software solution. Sessions must be recorded and ideally integrated with AI to make finding answers to specific questions easier and faster.

3.6.3 **Administrative Training:** Provide live training sessions for DSS/other South Dakota state employees that will become the administrators for the proposed software solution. Sessions must be recorded and ideally integrated with AI to make finding answers to specific questions easier and faster.

3.7 Other Features

The proposed software solution may have other features DSS may find useful. Describe each feature and its proposed use.

3.8 Hosting and Data Access Requirements

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

3.9 Single Sign-On Requirements

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

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

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

3.10 Onboarding/Provisioning Users

The offeror must describe how new users are onboarded/provisioned in the system using an external identity provider and provide an Identity/SSO/Login Design Document. The offeror must provide an automated process for onboarding and offboarding users or must provide a process that requires minimal manual steps.

3.11 Interfaces and Integration

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

3.12 Project Deliverables/Approach/Methodology

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

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

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

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

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

3.12.6 3.62.6 At BIT's discretion, any code changes made by the offeror, either during this project or thereafter, will be placed in the above test system first. It is at BIT's discretion if the code changes are applied by BIT or the offeror. If the code testing delays a project's timeline, a change management process should be followed, and the State will not be charged for this project change. If the test and production systems are to be hosted by the State, the schedule for the testing of the code changes is to be decided by BIT. Testing of emergency code changes will be scheduled by BIT based on the severity and resource availability.

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

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

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

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

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

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

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

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

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

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

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

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

3.12.16 Include in your submission details on your:

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

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

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

3.12.19 If the offeror's solution requires accounts allowing access to State systems, then the offeror must indicate the number of the offeror's staff or subcontractors that will require access, the level of access needed, and if these accounts will be used for remote access. These individuals will be required to use Multi-Factor Authentication (MFA). The State's costs in providing these accounts will be a consideration when assessing the cost of the offeror's solution. If the offeror later requires accounts that exceed the number of accounts that was originally indicated, the costs of those accounts will be borne by the offeror and not passed onto the State. All State security policies can be found in the Information Technology Security Policy (ITSP) as **Exhibit 1** to this RFP. The offeror should review the State's security policies regarding authorization, authentication, and, if relevant, remote access (See ITSP 230.67, 230.76, and 610.1). Use of Remote Access Devices (RAD) by contractors to access the State's system must be requested when an account is requested. The offeror should be aware that access accounts given to non-state employees, Non-State (NS) accounts, will be disabled if not used within 180 days. A NS account may be deleted after 30 days if it is not used.

3.12.20 The following testing may be required:

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

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

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

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

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

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

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

3.13 Non-Standard Hardware and Software

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

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

3.14 Background Checks

The offeror must include the following statement in its proposal:

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

3.15 Security and Vendor Questionnaire

The offeror must submit the completed Security and Vendor Questionnaire which is attached as **Attachment C**. These questions may be used in the proposal evaluation. It is preferred that the offeror’s response to these questions is provided as a separate document from the RFP response. If the offeror will be hosting the solution, the file name must be “(Your Name) Hosted Security and Vendor Questions Response”. If the solution will be hosted by the State, the file must be named “(Your Name) Security and Vendor Questions Response State Hosted”. If the solution is not a hosted solution, the file name must be “(Your Name) Security and Vendor Questions Response”. If there are multiple non-hosted solutions, please provide some designation in the file name that indicates which proposal it goes to. This document cannot be a scanned document but must be an original. If the offeror elects to make the Security and Vendor Questions part of its response, the questions must be clearly indicated in the proposal’s Table of Contents. A single numbering system must be used throughout the proposal.

4.0 PROPOSAL REQUIREMENTS AND COMPANY QUALIFICATIONS

4.1 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.

4.2 **Offeror's Contacts**: Offerors and their agents (including subcontractors, employees, consultants, or anyone else acting on their behalf) must direct all of their questions or comments regarding the RFP, the evaluation, etc. to the buyer of record indicated on the first page of this RFP. Offerors and their agents may not contact any state employee other than the buyer of record regarding any of these matters during the solicitation and evaluation process. Inappropriate contacts are grounds for suspension and/or exclusion from specific procurements. Offerors and their agents who have questions regarding this matter should contact the buyer of record.

4.3 Provide the following information related to at least three previous and current service/contracts, performed by the offeror's organization, which are similar to the requirements of this RFP.

4.3.1 Name, address and telephone number of client/contracting agency and a representative of that agency who may be contacted for verification of all information submitted;

4.3.2 Dates of the service/contract; and

4.3.3 A brief, written description of the specific prior services performed and requirements thereof.

4.4 The offeror must be required to submit a copy of their most recent independently audited financial statements.

4.5 If an offerors proposal is not accepted by the State, the proposal will not be reviewed/evaluated. Examples include: Proposal was not received on time. Proposal was not signed. Electronic file was not provided.

5.0 PROPOSAL RESPONSE FORMAT

5.1 Only a PDF copy shall be submitted via SFTP folder.

5.1.1 The proposal should be page numbered and should have an index and/or a table of contents referencing the appropriate page number.

5.2 All proposals must be organized and tabbed with labels for the following headings:

5.2.1 **RFP Form**. The State's Request for Proposal form (1st page of RFP) completed and signed.

5.2.2 **Executive Summary.** The one-to-two-page executive summary is to briefly describe the offeror's proposal. This summary should highlight the major features of the proposal. It must indicate any requirements that cannot be met by the offeror. 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.

5.2.3 **Detailed Response.** This section should constitute the major portion of the proposal and must contain at least the following information:

5.2.3.1 A complete narrative of the offeror's assessment of the work to be performed, the offeror's ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the offeror's understanding of the desired overall performance expectations.

5.2.3.2 A specific point-by-point response, in the order listed, to each requirement in the RFP. The response should identify each requirement being addressed as enumerated in the RFP.

5.2.3.3 A clear description of any options or alternatives proposed.

5.2.3.4 Completed Security and Vendor Questionnaire.

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

See section 7.0 for more information related to the cost proposal.

6.0 PROPOSAL EVALUATION AND AWARD PROCESS

6.1 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:

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

6.1.2 Resources available to perform the work, including any specialized services, within the specified time limits for the project;

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

6.1.4 Proposed project management techniques;

6.1.5 Ability and proven history in handling special project constraints;

6.1.6 Cost proposal; and

6.1.7 Availability to the project locale;

6.1.8 Familiarity with the project locale.

6.2 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.

6.3 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.

6.4 The State reserves the right to reject any or all proposals, waive technicalities, and make award(s) as deemed to be in the best interest of the State of South Dakota.

6.5 **Award:** The requesting agency and the highest ranked offeror shall mutually discuss and refine the scope of services for the project and shall negotiate terms, including compensation and performance schedule.

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

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

6.5.3 Only the response of the vendor awarded work becomes public. Responses to work orders for vendors not selected and the evaluation criteria and scoring for all proposals are not public. Vendors may submit a redacted copy with the full proposal as stated in Section 1.12 Proprietary Information. SDCL 1-27-1.5 and See SDCL 1-27-1.5 and 1-27-1.6.

7.0 COST PROPOSAL

Please use the Cost Proposal Template (**Attachment D**) provided to submit the information for this section. Vendors may submit multiple cost proposals. If the provided template is not appropriate for your proposal, please contact anthony.hardy@state.sd.us.

7.1 The vendor may submit cost proposals either in a breakdown of a proposed fixed contract amount or by hourly rate for professional services. Vendors may submit multiple cost proposals. If the licensing model for the proposed software solution has tiers based on the number of agents, number of visitors, number of locations, or other tier-based structure, please include pricing and tier requirements for the various tiers.

7.1.1 Use the following information for the first cost proposal: For the initial pilot at our largest location, the DSS One Stop in Sioux Falls, we expect between 150-160 visitors per day and approximately 200 agents.

7.1.2 If a Government Cloud (or similar) hosting option is available, please provide pricing proposals with and without this option.

7.1.3 For additional cost proposals, please include tier breaks and consider the information below for DSS's larger locations.

7.1.3.1	Aberdeen, SD:	Visitors/day: 40	Agents: 40
7.1.3.2	Huron, SD:	Visitors/day: 40	Agents: 40
7.1.3.3	Pierre, SD:	Visitors/day: 40	Agents: 40
7.1.3.4	Rapid City, SD:	Visitors/day: 80	Agents: 139

7.2 Professional services such as training, support, implementation, or configuration services (or other) must be separate line items.

7.3 As described above in Length of Contract, the length of the contract for the proposed software solution will be for approximately a one-year period of time with the opportunity to renew the contract annually with the option of four (3) one (1) year extensions. If the offeror expects cost increases in subsequent years, increase must be clearly identified for each year.

ATTACHMENT A

DSS Purchase Order #:25SC08 _ _ _ _
Consultant Contract #: 25-0800- _ _ _

STATE OF SOUTH DAKOTA
DEPARTMENT OF SOCIAL SERVICES
OFFICE OF THE SECRETARY

Consultant Contract
For Consultant Services
Between

State of South Dakota
Department of Social Services
OFFICE OF THE SECRETARY
700 Governors Drive
Pierre, SD 57501-2291

Referred to as Consultant	Referred to as State

The State hereby enters into a contract (the "Agreement" hereinafter) for consultant services with the Consultant. While performing services hereunder, Consultant is an independent consultant and not an officer, agent, or employee of the State of South Dakota.

1. CONSULTANT'S South Dakota Vendor Number is   . Upon execution of agreement, Consultant will provide the State with Consultant's Employer Identification Number or Federal Tax Identification Number.

2. PERIOD OF PERFORMANCE
   A. This Agreement shall be effective as of May 1, 2025 and shall end on May 31, 2026, unless sooner terminated pursuant to the terms hereof.

   B. Agreement is the result of request for proposal process, RFP #_____

3. PROVISIONS:
   A. The Purpose of this Consultant contract is:
      1.

      2. Does this Agreement involve Protected Health Information (PHI)? YES ( ) NO ( )
      If PHI is involved, a Business Associate Agreement must be attached and is fully incorporated herein as part of the Agreement (refer to attachment).

      3. The Consultant WILL ( ) WILL NOT ( ) use state equipment, supplies or facilities.

      4. If WILL is indicated above, the following state equipment, supplies, or facilities will be used.

   B. The Consultant agrees to perform the following services (add an attachment if needed):
      1.

   C. The State agrees to:
      1.

      2. Make payment for services upon satisfactory completion of services and receipt of bill. Payment will be in accordance with SDCL 5-26-2.

      3. Will the State pay Consultant expenses as a separate item?

YES ( ) NO (X)
If YES, expenses submitted will be reimbursed as identified in this Agreement.

D. The TOTAL CONTRACT AMOUNT will not exceed **$.**

4. BILLING:
Consultant agrees to submit a bill for services within (30) days following the month in which services were provided. Consultant will prepare and submit a monthly bill for services. Consultant agrees to submit a final bill within 30 days of the Agreement end date to receive payment for completed services. If a final bill cannot be submitted in 30 days, then a written request for extension of time and explanation must be provided to the State.

5. TECHNICAL ASSISTANCE:
The State agrees to provide technical assistance regarding Department of Social Services rules, regulations and policies to the Consultant and to assist in the correction of problem areas identified by the State's monitoring activities.

6. LICENSING AND STANDARD COMPLIANCE:
The Consultant agrees to comply in full with all licensing and other standards required by Federal, State, County, City or Tribal statute, regulation or ordinance in which the service and/or care is provided for the duration of this Agreement. The Consultant will maintain effective internal controls in managing the federal award. Liability resulting from noncompliance with licensing and other standards required by Federal, State, County, City or Tribal statute, regulation or ordinance or through the Consultant's failure to ensure the safety of all individuals served is assumed entirely by the Consultant.

7. ASSURANCE REQUIREMENTS:
(For Federally funded contracts only). The Consultant agrees to abide by all applicable provisions of the following: Byrd Anti Lobbying Amendment (31 USC 1352), Executive orders 12549 and 12689 (Debarment and Suspension), Drug-Free Workplace, Executive Order 11246 Equal Employment Opportunity, Title VI of the Civil Rights Act of 1964, Title VIII of the Civil Rights Act of 1968, Section 504 of the Rehabilitation Act of 1973, Title IX of the Education Amendments of 1972, Drug Abuse Office and Treatment Act of 1972, Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970, Age Discrimination Act of 1975, Americans with Disabilities Act of 1990, Pro-Children Act of 1994, Hatch Act, Health Insurance Portability and Accountability Act (HIPAA) of 1996 as amended, Clean Air Act, Federal Water Pollution Control Act, Charitable Choice Provisions and Regulations, Equal Treatment for Faith-Based Religions at Title 28 Code of Federal Regulations Part 38, the Violence Against Women Reauthorization Act of 2013 and American Recovery and Reinvestment Act of 2009, as applicable; and any other nondiscrimination provision in the specific statute(s) under which application for Federal assistance is being made; and the requirements of any other nondiscrimination statute(s) which may apply to the award.

8. COMPLIANCE WITH EXECUTIVE ORDER 2020-01:
Executive Order 2020-01 provides that for consultants, vendors, suppliers or subcontractors with five (5) or more employees who enter into a contract with the State that involves the expenditure of one hundred thousand dollars ($100,000) or more, by signing this Agreement Consultant 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. Consultant 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.

9. COMPLIANCE WITH SDCL ch 5-18A:
Consultant certifies and agrees that the following information is correct:

The bidder or offeror is not an organization, association, corporation, partnership, joint venture, limited partnership, limited liability partnership, limited liability company, or other entity or business association, including all wholly-owned subsidiaries, majority-owned subsidiaries, parent companies, or affiliates, of those entities or business associations, regardless of their principal place of business, which is ultimately owned or controlled, directly or indirectly, by a foreign parent entity from, or the government of, the People's Republic of China, the Republic of Cuba, the Islamic Republic of Iran, the Democratic People's Republic of Korea, the Russian Federation, or the Bolivarian Republic of Venezuela.

It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the purchasing agency to reject the bid or response submitted by the bidder or offeror on this project and terminate any contract awarded based on the bid or response, and further would be cause to suspend and debar a business under SDCL § 5-18D-12.

The successful bidder or offeror further agrees to provide immediate written notice to the purchasing agency if during the term of the contract it no longer complies with this certification and agrees such noncompliance may be grounds for contract termination and would be cause to suspend and debar a business under SDCL § 5-18D-12.

10. CERTIFICATION OF NO STATE LEGISLATOR INTEREST:
Consultant (i) understands neither a state legislator nor a business in which a state legislator has an ownership interest may be directly or indirectly interested in any contract with the State that was authorized by any law passed during the term for which that legislator was elected, or within one year thereafter, and (ii) has read South Dakota Constitution Article 3, Section 12 and has had the opportunity to seek independent legal advice on the applicability of that provision to this Agreement. By signing this Agreement, Consultant hereby certifies that this Agreement is not made in violation of the South Dakota Constitution Article 3, Section 12.

11. RETENTION AND INSPECTION OF RECORDS:
The Consultant agrees to maintain or supervise the maintenance of records necessary for the proper and efficient operation of the program, including records and documents regarding applications, determination of eligibility (when applicable), the provision of services, administrative costs, statistical, fiscal, other records, and information necessary for reporting and accountability required by the State. The Consultant shall retain such records for a period of six years from the date of submission of the final expenditure report. If such records are under pending audit, the Consultant agrees to hold such records for a longer period upon notification from the State. The State, through any authorized representative, will have access to and the right to examine and copy all records, books, papers or documents related to services rendered under this Agreement. State Proprietary Information retained in Consultant's secondary and backup systems will remain fully subject to the obligations of confidentiality stated herein until such information is erased or destroyed in accordance with Consultant's established record retention policies.

All payments to the Consultant by the State are subject to site review and audit as prescribed and carried out by the State. Any over payment of this Agreement shall be returned to the State within thirty days after written notification to the Consultant.

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

13. TERMINATION:
This Agreement may be terminated by either party hereto upon thirty (30) days written notice. In the event the Consultant breaches any of the terms or conditions hereof, this Agreement may be terminated by the State at any time, with or without notice. Upon termination of this Agreement, all accounts and payments shall be processed according to financial arrangements set forth herein for services rendered to date of termination. If termination for breach is effected by the State, any payments due to Consultant at the time of termination may be adjusted to cover any additonal costs to the State as a result of Consultant's breach. Upon termination the State may take over the work and may award another party a contract to complete the work contemplated by this Agreement. If the State terminates for a breach by Consultant and it is determined that the Consultant was not at fault, then Consultant shall be paid for eligible services rendered and expenses incurred up to the date of termination.

    Any terms of this Agreement that would, by their nature or through the express terms of this Agreement, survive the expiration or termination of this Agreement shall so survive, including by not limited to the terms of sections 10, 11, 15, 23, 24, and 27.

14. 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 upon five day written notice. Consultant agrees that termination for any of these reasons is not a default by the State nor does it give rise to a claim against the State or any officer, agent or employee of the State and Consultant waives any claim against the same.

15. ASSIGNMENT AND AMENDMENTS:
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.

16. 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 resolved in the Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota.

17. THIRD PARTY BENEFICIARIES:
This agreement is intended to govern only the rights and interests of the parties named herein. It is not intended to create, does not and may not be relied upon to create, any rights, substantive or procedural, enforceable at law in any matters, civil or criminal.

18. SUPERSESSION:
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.

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

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

21. 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 the Division being contracted with on behalf of the State, and by the Consultant, 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.

22. SUBCONSULTANTS:
Consultant may not use subconsultants to perform the services described herein without the express prior written consent of the State. Consultant will include provisions in its subcontracts requiring its subconsultants to comply with the applicable provisions of this Agreement, to indemnify the State, and to provide insurance coverage in a manner consistent with this Agreement. Consultant will cause its subconsultants, agents, and employees to comply with applicable federal, tribal, state, and local laws, regulations, ordinances, guidelines, permits and other standards 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 subconsultants. Consultant shall assist in the vetting process.

23. STATE’S RIGHT TO REJECT:
The State reserves the right to reject any person from performing services under this Agreement who the State believes would be detrimental to the services, presents insufficient skills, presents inappropriate behavior or is considered by the State to be a security risk.

24. INDEMNIFICATION:
Consultant agrees to indemnify the State of South Dakota, its officers, agents, and employees, from and against all claims or proceedings for actions, suits, damages, liabilities, other losses or equitable relief that may arise at least in part as a result of an act or omission in performing services under this Agreement. Consultant shall defend the State of South Dakota, its officers, agents, and employees against any claim, including any claim, action, suit, or other proceeding related to the claim. Consultant’s obligation to indemnify includes the payment of attorney fees and other costs of defense. In defending the State of South Dakota, its officers, agents, and employees, Consultant shall engage other professionals, subject to the written approval of the State which shall not be unreasonably withheld. Notwithstanding the foregoing, the State may, in its sole discretion and at the expense of Consultant, engage attorneys and other professionals to defend the State of South Dakota, its officers, agents, and employees, or to assist Consultant in the defense. This section does not require Consultant to be responsible for or defend against claims or proceedings for damages, liabilities, losses or equitable relief arising solely from errors or omissions of the State, its officers, agents or employees.

25. INSURANCE:
At all times during the term of this Agreement, Consultant shall obtain and maintain in force insurance coverage of the types and with the limits as follows:

A. Commercial General Liability Insurance:
Consultant 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. The insurance policy shall name the State of South Dakota, its officers and employees, as additional insureds, but liability coverage is limited to claims not barred by sovereign immunity. The State of South Dakota, its officers and employees do not hereby waive sovereign immunity for discretionary conduct as provided by law.

B. Professional Liability Insurance or Miscellaneous Professional Liability Insurance:
Consultant agrees to procure and maintain professional liability insurance or miscellaneous professional liability insurance with a limit not less than one million dollars $1,000,000.

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

D. Worker's Compensation Insurance:
Consultant shall procure and maintain Workers' Compensation and employers' liability insurance as required by South Dakota or federal law.

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

26. CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY, AND VOLUNTARY EXCLUSION:
Consultant certifies, by signing this Agreement, 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. Consultant 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.

27. CONFLICT OF INTEREST:
Consultant agrees to establish safeguards to prohibit employees or other persons from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain as contemplated by SDCL 5-18A-17 through 5-18A-17.6. Any potential conflict of interest must be disclosed in writing. In the event of a conflict of interest, the Consultant expressly agrees to be bound by the conflict resolution process set forth in SDCL 5-18A-17 through 5-18A-17.6.

28. CONFIDENTIALITY OF INFORMATION:
For the purpose of this Agreement, "Confidential Information" shall include all information, regardless of its format, disclosed to Consultant by the State and all information, regardless of its format, obtained by Consultant through the provisions of services as contemplated by this Agreement. Consultant, and any person or entity affiliated with Consultant 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. Consultant, and any person or entity affiliated with Consultant 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, by contract, to obligations of confidentiality at least as strict as those set out in this Agreement and who have a need to know such information and who have been instructed that such information is or may be confidential under state or federal law. Consultant, and any person or entity affiliated with Consultant 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. Consultant, and any person or entity affiliated with Consultant shall protect the confidentiality of the State's information from the time of receipt to the time that such information is either returned to the State or destroyed to the extent that it cannot be recalled or reproduced.

Confidential Information shall not include information that: (i) was in the public domain at the time it was disclosed to Consultant or to any person or entity affiliated with Consultant; (ii) was known to Consultant, or to any person or entity affiliated with Consultant, without restriction at the time of disclosure from the State; (iii) was disclosed with the prior written approval of State's officers or employees having authority to disclose such information; (iv) was independently developed by Consultant, or by any person or entity affiliated with Consultant, without the benefit or influence of the State's information; or (v) becomes known to Consultant, or to any person or entity affiliated with Consultant, without restriction, from a source not connected to the State of South Dakota.

Confidential Information can include, but is not limited to, 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. Consultant understands that this information may be confidential and protected under state or federal law. Consultant agrees to immediately notify the State if the information is disclosed, either intentionally or inadvertently.

If work assignments performed in the course of this Agreement require additional security requirements or clearance, Consultant 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.

Consultant will enforce the terms of this Confidentiality Provision to its fullest extent.

Consultant 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.
Consultant 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, Consultant agrees to return to the State, at Consultant's cost, any Confidential Information or documentation maintained by Consultant regarding the services provided hereunder in a format readily useable by the State as mutually agreed by Consultant and State.

29. REPORTING PROVISION:
Consultant 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 Consultant, or the State of South Dakota or its officers, agents or employees to liability. Consultant shall report any such event to the State immediately upon discovery.

Consultant'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. Consultant'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 Consultant to report any event to law enforcement or other entities under the requirements of any applicable law.

30. DAVIS-BACON ACT:
When required by Federal program legislation, all prime construction contracts in excess of $2,000 awarded by non-Federal entities must include a provision for compliance with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction").

31. COMPLIANCE WITH 40 U.S.C. 3702 AND 3704:
Where applicable, all contracts awarded by the non-Federal entity in excess of $100,000 that involve the employment of mechanics or laborers must include a provision for compliance with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5).

32. FUNDING AGREEMENT AND "RIGHTS TO INVENTION":
If the Federal award meets the definition of "funding agreement" under 37 CFR §401.2 (a) and the Consultant wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the Consultant must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

33. 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 any 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.

34. SOVEREIGN IMMUNITY:
Nothing in this Agreement is intended to constitute a waiver of sovereign immunity by or on behalf of the State of South Dakota, its agencies, officers, or employees.

35. WAIVER OF BREACH:
The waiver by either party of a breach or violation of any provision of this Agreement shall not operate as, or be construed to be, a waiver of any subsequent breach of the same or other provisions in this Agreement.

36. HEADINGS:
The headings in this Agreement are for convenience and reference only and shall not govern, limit, modify or in any manner affect the scope, meaning, or intent of the provisions of this Agreement.

37. AUTHORITY TO EXECUTE:
Consultant represents and warrants that:

A. Consultant is a corporation duly incorporated, validly existing and in good standing under the laws of its state of incorporation and has all requisite corporate power and authority to execute, deliver and perform its obligations under this Agreement;

B. The execution, delivery and performance of this Agreement has been duly authorized by Consultant and no approval, authorization or consent of any governmental or regulatory agency is required to be obtained in order for Consultant to enter into this Agreement and perform its obligations under this Agreement;

C. Consultant is duly authorized to conduct business in and is in good standing in each jurisdiction in which Consultant will conduct business in connection with this Agreement; and

D. Consultant has obtained all licenses, certifications, permits, and authorizations necessary to perform the services under this Agreement and currently is in good standing with all regulatory agencies that regulate any or all aspects of Consultant's performance of the services. Consultant will maintain all required certifications, licenses, permits, and authorizations during the term of this Agreement at its own expense.

38. AUTHORIZED SIGNATURES**:**
In witness hereto, the parties signify their agreement by affixing their signatures hereto.

NO SIGNATURE REQUIRED AT THIS TIME

Consultant Signature Date

Consultant Printed Name

State - DSS Division Director Date

State - DSS Chief Financial Officer Jason Simmons Date

State – DSS Cabinet Secretary Matthew K. Althoff Date

State Agency Coding:

ALN # ____________ ____________ ____________ ____________
Company ____________ ____________ ____________ ____________
Account ____________ ____________ ____________ ____________
Center Req ____________ ____________ ____________ ____________
Center User ____________ ____________ ____________ ____________
Dollar Total ____________ ____________ ____________ ____________

DSS Program Contact Person ________________________________
Phone ____________

DSS Fiscal Contact Person Contract Accountant
Phone 605 773-3586

Consultant Program Contact Person ________________________________
Phone ____________
Consultant Program Email Address ____________

Consultant Fiscal Contact Person ________________________________
Phone ________________________________
Consultant Fiscal Email Address ________________________________

SDCL 1-24A-1 states that a copy of all consulting contracts shall be filed by the State agency with the State Auditor within five days after such contract is entered into and finally approved by the contracting parties. For further information about consulting contracts, see the State Auditor's policy handbook.

CERTIFICATION REQUIRED BY SDCL ch 5-18A

Section 1 Definitions. The words used in this Certification shall mean:

1.1. "Prohibited Entity," an organization, association, corporation, partnership, joint venture, limited partnership, limited liability partnership, limited liability company, or other entity or business association, including all wholly-owned subsidiaries, majority-owned subsidiaries, parent companies, or affiliates, of those entities or business associations, regardless of their principal place of business, which is ultimately owned or controlled, directly or indirectly, by a foreign parent entity from, or the government of, the People's Republic of China, the Republic of Cuba, the Islamic Republic of Iran, the Democratic People's Republic of Korea, the Russian Federation, or the Bolivarian Republic of Venezuela;

1.2. "Purchasing agency," any governmental body or officer authorized by law, administrative rule, or delegated authority, to enter into contracts;

1.3. "Contract," any type of agreement, regardless of what the agreement may be called, for the procurement of supplies, services, or construction;

Section 2. Certification. The undersigned hereby certifies to the State of South Dakota that:

2.1. The undersigned is not a Prohibited Entity.

2.2 If at any time after making this certification the undersigned becomes a Prohibited Entity, the undersigned will provide immediate written notice to all purchasing agencies with whom the undersigned has a Contract. The undersigned understands and agrees that if the undersigned becomes a Prohibited Entity, agencies may terminate any Contract with the undersigned.

2.3 The undersigned acknowledges and agrees that agencies have the right to terminate a Contract with any entity that submits a false certification, and that a false certification or failure to provide written notification to purchasing agencies that an entity has become a prohibited entity is cause to suspend or debar a business under SDCL § 5-18D-12.

____
Company

NO SIGNATURE REQUIRED AT THIS TIME

Title　　　　　　　　Signature　　　　　　　　Date

ATTACHMENT B

Bureau of Information and Telecommunications
Required IT Contract Terms

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

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

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

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

Section I. Confidentiality of Information

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

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

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

Section II. Cyber Liability Insurance

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

Section III. Rejection or Ejection of Vendor

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

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

Section IV. Domain Name Ownership

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

Section V. Software Functionality and Replacement

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

The Vendor agrees that:

A. If, in the opinion of the State, the Vendor reduces or replaces the functionality contained in the licensed product and provides this functionality as a separate or renamed product, the State will be entitled to license such software product at no additional license or maintenance fee.

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

Section VI. Service Bureau

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

Section VII. Federal Intellectual Property Bankruptcy Protection Act

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

Section VIII. Non-Disclosure and Separation of Duties

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

Section IX. Cessation of Business

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

Section X. Legal Requests for Data

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

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

Section XI. eDiscovery

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

Section XII. Audit Requirements

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

Section XIII. Annual Risk Assessment

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

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

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

Section XIV. Independent Audit

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

Section XV. Service Level Agreements

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

Section XVI. Access Attempts

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

Section XVII. Access to State Data

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

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

Section XVIII. Password Protection

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

Section XIX. Provision of Data

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

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

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

Section XX. Threat Notification

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

Section XXI. Security Incident Notification for Non-Health Information

The Vendor will implement, maintain, and update Security Incident procedures that comply with all State standards and Federal and State requirements. A Security Incident is a violation of any BIT security or privacy policies or contract agreements involving sensitive information, or the imminent threat of a violation. The BIT security policies can be found in the Information Technology Security Policy (“ITSP”) attached as BIT Attachment 1. The State requires notification of a Security Incident involving any of the State’s sensitive data in the Vendor’s possession. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party. The parties agree that, to the extent probes and reconnaissance scans common to the industry constitute Security Incidents, this Agreement constitutes notice by the Vendor of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State will be required. Probes and scans include, without limitation, pings and other broadcast attacks in the Vendor’s firewall, port scans, and unsuccessful log-on attempts, if such probes and reconnaissance scans do not result in a Security Incident as defined above. Except as required by other legal requirements the Vendor will only provide notice of the incident to the State. The State will determine if notification to the public will be by the State or by the Vendor. The method and content of the notification of the affected parties will be coordinated with, and is subject to approval by the State, unless required otherwise by legal requirements. If the State decides that the Vendor will be distributing, broadcasting to or otherwise releasing information on the Security Incident to the news media, the State will decide to whom the information will be sent, and the State must approve the content of any information on the Security Incident before it may be distributed, broadcast, or otherwise released. The Vendor must reimburse the State for any costs associated with the notification, distributing, broadcasting, or otherwise releasing information on the Security Incident.

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

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

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

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

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

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

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

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

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

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

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

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

Section XXIII. Security Incidents for Protected Health Information

Security Incident means the successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system as defined in 45 CFR 164.304. The Vendor must alert the State contact within 12 hours of a Security Incident and provide daily updates to the BIT contact at their request. The Parties agree that this alert does not affect the Vendor's obligations under the Business Associate Agreement or the requirements of 45 CFR 164.410. The Parties agree that, to the extent probes and reconnaissance scans common to the industry constitute a Security Incident, this Agreement constitutes notice by the Vendor of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State will be required. Probes and scans include, without limitation, pings, and other broadcast attacks in the Vendor's firewall, port scans, and unsuccessful log-on attempts, if such probes and reconnaissance scans do not result in a Security Incident as defined above. The State can require the Vendor to conduct a review or investigation within the scope and methodology determined by the State. At the State's discretion, the review or investigation may be performed by a third party at the Vendor's expense.

Notwithstanding any other provision of this Agreement and in addition to any other remedies available to the State under law or equity, in the event the investigation or review determines that the Vendor is responsible for the Security Incident, and where the State incurs any costs in the investigation, review, or remediation of the Security Incident, the Vendor must reimburse the State in full for all such costs. Costs include, but are not limited to, providing notification to regulatory agencies or other entities as required by law or contract. In the event the investigation or review determines that the Vendor is responsible for the Security Incident, the Vendor must also pay all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident, and all costs associated with the remediation of the Vendor's services or product(s).

Section XXIV. Adverse Event

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

Section XXV. Browser

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

Section XXVI. Security of Code

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

Section XXVII. Security Acknowledgment Form

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

Section XXVIII. Background Investigations

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

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

Section XXIX. Information Technology Standards

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

Section XXX. Product Usage

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

Section XXXI. Security

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

By signing this Agreement, the Vendor warrants that:

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

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

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

C. All members of the development team have been successfully trained in secure programming techniques.

D. A source code control system will be used that authenticates and logs the team member associated with all changes to the software baseline and all related configuration and build files.

E. State access to the source code will be allowed to ensure State security standards, policies, and best practices which can be found at https://bit.sd.gov/bit?id=bit_standards_overview.

F. The Vendor will fully support and maintain the Vendor's application on platforms and code bases (including but not limited to: operating systems, hypervisors, web presentation layers, communication protocols, security products, report writers, and any other technologies on which the application depends) that are still being supported, maintained, and patched by the applicable third parties owning them. The Vendor may not withhold support from the State for this application nor charge the State additional fees as a result of the State moving the Vendor's application to a new release of third-party technology if:

   1. The previous version of the third-party code base or platform is no longer being maintained, patched, and supported; and
   2. The new version to which the State moved the application is actively maintained, patched, and supported.

If there are multiple versions of the applicable code base or platform(s) supported by the third party in question, the Vendor may limit its support and maintenance to any of the applicable third-party code bases or platforms.

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

Section XXXII. Security Scanning

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

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

Section XXXIII. Secure Product Development

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

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

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

Section XXXIV. Malicious Code

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

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

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

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

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

Section XXXVI. Movement of Product

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

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

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

Section XXXVIII. Load Balancing

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

Section XXXIX. Backup Copies

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

A. The State maintains possession of the backup copies.
B. The backup copies are used only as bona fide backups.

Section XL. Use of Abstraction Technologies

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

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

Section XLI. Scope of Use

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

Section XLII. License Agreements

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

Section XLIII. Web and Mobile Applications

A. The Vendor's application is required to:

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

14. have an opening screen that states, in an easy-to-read font, that the application is gathering or accessing health or medical information and the user's privacy is not protected by federal regulations if any health or medical information is gathered or accessed by the application that is not protected by HIPAA and HITECH rules and regulations, and
15. any application to be used on a mobile device must be password protected.

B. The Vendor is required to disclose all:

1. functionality,
2. device and functional dependencies,
3. third party libraries used,
4. methods user data is being stored, processed, or transmitted,
5. methods used to notify the user how their data is being stored, processed, or transmitted,
6. positive actions required by the user to give permission for their data to be stored, processed and or transmitted,
7. methods used to record the user's response(s) to the notification that their data is being stored, processed, or transmitted,
8. methods used to secure the data in storage, processing, or transmission,
9. forms of authentication required for a user to access the application or any data it gathers stores, processes and or transmits,
10. methods used to create and customize existing reports,
11. methods used to integrate with external data sources,
12. methods used if integrates with public cloud provider,
13. methods and techniques used and the security features that protect data, if a public cloud provider is used, and
14. formats the data and information uses.

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

Section XLIV. Intended Data Access Methods

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

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

Section XLV. Application Programming Interface

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

Section XLVI. Access to Source and Object Code

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

Section XLVII. Data Location and Offshore Services

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

Section XLVIII. Vendor's Software Licenses

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

Section XLIX. Vendor Training Requirements

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

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

Section L. Data Sanitization

At the end of the project covered by this Agreement the Vendor, and Vendor's subcontractors, agents, assigns, and affiliated entities will return the State Data or securely dispose of all State Data in all forms, this can include State Data on media such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs. This State Data must be permanently deleted by either purging the data or destroying the medium on which the State Data is found according to the methods given in the most current version of NIST 800-88. Certificates of Sanitization for Offsite Data (See bit.sd.gov/vendor/default.aspx for copy of certificate) must be completed by the Vendor and given to the State contact. The State will review the completed

Certificates of Sanitization for Offsite Data. If the State is not satisfied by the data sanitization then the Vendor will use a process and procedure that does satisfy the State.

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

Section LI. Banned Hardware and Software

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

Section LII. Hardware Passwords

Any hardware installed on the State network must have any default passwords changed when the hardware is configured to meet State password requirements in the Information Technology Security Policy, see BIT Attachment 1.

Section LIII. Use of Portable Devices

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

Section LIV. Remote Access

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

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

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

Section LV. Data Encryption

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

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

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

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

A. The Vendor will implement and maintain appropriate administrative, technical, and organizational security measures to safeguard against unauthorized access, disclosure, use, or theft of Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI), or any information that is confidential under applicable federal, state, or international law, rule, regulation, or ordinance. Such security measures will be in accordance with recognized industry practice and not less protective than the measures the Vendor applies to its own non-public data.

B. The Vendor will not copy, disclose, retain, or use State Data for any purpose other than to fulfill its obligations under this Agreement.

C. The Vendor will not use State Data for the Vendor's own benefit and will not engage in data mining of State Data or communications, whether through automated or manual means, except as specifically and expressly required by law or authorized in writing by the State through a State employee or officer specifically authorized to grant such use of State Data.

Section LVII. Third Party Hosting

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

Section LVIII. Securing of Data

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

Section LIX. Security Processes

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

Section LX. Import and Export of Data

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

Section LXI. System Upgrades

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

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

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

Section LXIII. Banned Services

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

Section LXIV. Multifactor Authentication for Hosted Systems

If the Vendor is hosting on their system or performing Software as a Service where there is the potential for the Vendor or the Vendor’s subcontractor to see protected State Data, then Multifactor Authentication (MFA) must be used before this data can be accessed. The Vendor’s

MFA, at a minimum must adhere to the requirements of *Level 2 Authentication Assurance for MFA* as defined in NIST 800-63.