

**STATE OF SOUTH DAKOTA
INFORMATION TECHNOLOGY (IT) RFP
(Bureau of Human Resources and Administration
500 E Capitol Ave, Pierre, SD 57501)**

South Dakota State Employee Health Plan Medical Claims Audit

PROPOSALS ARE DUE NO LATER THAN October 23, 2026

RFP #: 26RFP19878

STATE POC: State of South Dakota,
Bureau of Human Resources &
Administration

EMAIL:
Peggy.Canter@state.sd.us

READ CAREFULLY

FIRM NAME: _____ AUTHORIZED SIGNATURE: _____

ADDRESS: _____ TYPE OR PRINT NAME: _____

CITY/STATE: _____ TELEPHONE NO: _____

ZIP (9 DIGITS): _____ FAX NO: _____

E-MAIL: _____

PRIMARY CONTACT INFORMATION

CONTACT NAME: Peggy Canter

TELEPHONE NO: 605-773-4099

FAX NO: _____

E-MAIL: Peggy.Canter@state.sd.us

1 General Information

1.1 Purpose of Request for Proposal (RFP)

1.1.1 Background:

Wellmark Blue Cross Blue Shield of South Dakota ("Wellmark") has been administering the State's self-funded medical and pharmacy plans since July 1, 2021. Approximately 12,150 State employees and COBRA participants enrolled in four (4) State of South Dakota State Employee Health Plans ("SDSEHP") which includes 2 low-deductible Preferred Provider Organization ("PPO") plans and 2 high-deductible plans which offer a Health Savings Account ("HSA"). The total number of plan participants including spouses and dependent children is approximately 26,800. As of May 1, 2026, 65.00% of plan members were enrolled in the high-deductible health plans and 35.00% were enrolled in the low-deductible plans. Annual paid claims volume is approximately 314,300 medical claims and 282,700 pharmacy claims. For Fiscal Year 2026 (ended on June 30, 2026), the SDSEHP paid a total of approximately \$160 million in total health plan costs (medical claims, prescription drug claims, and administrative fees), of which approximately \$108 million was for medical claims alone.

The Bureau of Human Resources & Administration ("BHRA") is soliciting proposals from vendors who can conduct a performance review of medical claims processing performed by Wellmark. The auditor selected through this RFP process will be required to execute a Non-Disclosure Agreement ("NDA") with Wellmark.

1.1.2 Goals and Objectives

- a. Perform the Medical Claims Audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the U.S. Government Accountability Office.
- b. Follow industry-standard methodologies for medical and pharmacy claims auditing, including statistically valid sampling techniques.
- c. Maintain auditor independence, appropriate qualifications, and relevant experience in health plan and claims audits.
- d. Provide documentation and work papers sufficient for the State to validate findings, conclusions, and recommended corrections.
- e. Comply with any additional federal or state requirements applicable to the State Health Plan, if relevant (e.g., OMB Uniform Guidance, only if federal funds or requirements are triggered).

- f. Verify that claims are being processed in compliance with the State's plan Provisions;
- g. Verify Wellmark procedures and controls, and negotiated network provider rates;
- h. Measure the quality and timeliness of Wellmark's claims processing performance;
- i. Assess the reliability of Wellmark's self-reported results for performance guarantees; and
- j. Assess the accuracy of claims data provided by Wellmark to the State.

1.1.3 Description of Components or Phases:

The work product is for three (3) Audit Periods, each with one twelve (12) month period. Within the Audit Periods, each year will have a separate and distinct findings, reports and recommendations.

1.1.4 Scope of Components or Phases:

- **Audit Period 1 will be July 1, 2027 to June 30, 2028 (Fiscal Year 2028)**
- **Audit Period 2 will be July 1, 2028 to June 30, 2029 (Fiscal Year 2029)**
- **Audit Period 3 will be July 1, 2029 to June 30, 2030 (Fiscal Year 2030)**

1.2 Issuing Office and RFP Reference Number

The Bureau of Human Resources and Administration ("BHRA") is the issuing office for this document and all subsequent addenda relating to it, on behalf of the State of South Dakota ("State"). The reference number for this transaction is RFP#26RFP19878. This reference number must be referred to on all proposals, correspondence, and documentation relating to this RFP. For purposes of this RFP, the State's centralized IT agency, the Bureau of Information and Technology ("BIT"), must approve all IT related purchases.

1.3 Schedule of Activities (Subject to Change)

All deadlines in the Schedule of Activities are due by 11:59 p.m. CST. The Schedule of Activities for this RFP is as follows:

RFP Publication	September 28, 2026
Deadline for Letter of Intent to Respond	October 12, 2026
Deadline for Submission of Written Inquiries	October 12, 2026
Deadline for Responses to offeror Questions	October 21, 2026
Deadline for Proposal Submission	October 23, 2026
Evaluation of Proposals to Determine Short List (If required)	November 6, 2026
Discussions / Technical Review, if applicable	November 16, 2026
Deadline for Completion of Site Visits (If required)	November 9-13, 2026
Demonstrations and presentations (if required)	November 9-13, 2026
Proposal Revisions (if required)	November 30, 2026
Anticipated Award Decision/Contract Negotiation	December 7, 2026

1.4 Submitting a Proposal

All proposals must be completed and received by the Agency by the date and time indicated in **Section 1.3 Schedule of Activities**.

Proposals received after the Deadline for Proposal Submission will be late and ineligible for consideration.

All proposals must be signed, in ink or electronically, by a representative of the offeror who is legally authorized to bind the offeror to the proposal. Proposals that are not properly signed may be rejected. The offeror's proposal must be prepared pursuant to the requirements of **Section 5 Proposal Response Format** of this RFP.

The State will only accept electronic proposals via email.

Each offeror must provide an electronic version of the proposal. The electronic version should be provided in MS Word or in PDF format to Peggy.Canter@state.sd.us. The email, including attachments, must be limited to 20MB in size.

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

1.5 Certification Regarding Debarment, Suspension, Ineligibility, and Voluntary Exclusion – Lower Tier Covered Transactions

By signing and submitting this proposal, the offeror certifies that neither its principals are 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 any of the statements in this certification, the offeror shall attach an explanation to its offer.

1.6 Non-Discrimination Statement

The State of South Dakota requires that all contractors, vendors, and suppliers do 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 regarding race, color, creed, religion, age, sex, ancestry, national origin, or disability.

1.7 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.

1.8 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 a prohibited entity, regardless of its principal place of business, that is ultimately owned or controlled, directly or indirectly, by a foreign national, a foreign parent entity, or foreign government from China, Iran, North Korea, Russia, Cuba, or Venezuela, as defined by South Dakota Codified Law § 5-18A. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to reject the bid or response submitted by the bidder or offeror on this project and terminate any contract awarded based on the bid or response. The successful bidder or offeror further agrees to provide immediate written notice to the contracting executive branch agency if during the term of the contract it no longer complies with this certification and agrees such noncompliance may be grounds for contract termination and would be cause to suspend and debar a business under SDCL § 5-18D-12.

1.9 Modification or Withdrawal of Proposals

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

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

1.10 Questions Regarding RFP

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

Each offeror may submit questions via email concerning this RFP to obtain clarification of requirements. No questions will be accepted after the date and time indicated in the

above schedule of activities. Email questions to the email address listed above with the subject line "RFP#26RFP19878". The questions and their answers will be sent to all offerors that submitted Letters of Intent, submitted questions, or requested the questions and answers via email before the proposal submittal date and will be sent by the date and time indicated in the above calendar of events. Offeror may not rely on any other statements, either of a written or oral nature, that alter any specification or other term or condition of this RFP that have not originated from the SD RFP Project Contact. Offerors will be notified in the same manner as indicated above regarding any modifications to this RFP. Offerors and their agents may not contact any state employee other than the buyer of record regarding any of these matters during the solicitation and evaluation process. Inappropriate contacts are grounds for suspension and exclusion from specific procurements.

1.11 Prohibition on Solely AI-Generated Submissions

All questions, responses, and proposals submitted in response to this RFP must be thoroughly vetted, verified, and validated by the vendor's human staff. Submissions that are solely generated by Artificial Intelligence (AI) without substantive human review and oversight are strictly prohibited and may result in the disqualification of the proposal or rejection of the submitted questions.

1.12 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.

1.13 Length of Contract

The length of the contract will be for a term of three (3) year(s). The State will have the opportunity to renew the contract annually for up to two (2) additional one-year time extensions. The extension(s) will not be automatic.

1.14 Governing Law

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

1.15 Site Visit

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

1.16 Presentations/Demonstrations

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

1.17 Discussions

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

1.18 Technical Review

At the State's discretion, the State may require a technical review of the offeror based on the offeror's proposal and response to the Security and Vendor Questionnaire.

1.19 Negotiations

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

2 Standard Contract Terms and Conditions

Any contract or agreement resulting from this RFP #26RFP19878 will include the State's standard terms and conditions as listed below, the State's standard Information Technology ("IT") contract terms listed in Exhibit B, and any additional terms and conditions as negotiated by the parties. The offeror must indicate in its response any issue it has with specific contract terms. If the offeror does not indicate that there is an issue with a specific contract term, then the offeror will be deemed to have accepted the contract terms as written.

- 2.1** The Contractor will perform those services described in the Scope of Work, attached hereto as Section 3 of the RFP and by this reference incorporated herein.
- 2.2** The Contractor's services under this Agreement will start on July 1, 2027 and end on June 30, 2030 unless terminated sooner pursuant to the terms of the Agreement.
- 2.3** The State will have the option to renew this Agreement for two (2) additional one (1) year periods, under the same terms and conditions. If the State chooses to renew the Agreement, the State shall provide notice of intent to renew to the Contractor as mutually agreed upon prior to the end of the current Agreement term. If notice of intent to renew is given, the Agreement shall renew unless terminated by either party pursuant to the Termination Provision of this Agreement.

- 2.4** The Contractor will not use State equipment, supplies, or facilities. The Contractor will provide the State with its Employer Identification Number, Federal Tax Identification Number, or Social Security Number upon execution of this Agreement.
- 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 chapter 5-26.
- 2.6** The Contractor 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. The Contractor will 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. The Contractor'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, the Contractor will engage other professionals, subject to the written approval of the State which will not be unreasonably withheld. Notwithstanding the foregoing, the State may, in its sole discretion and at the expense of the Contractor, engage attorneys and other professionals to defend the State of South Dakota, its officers, agents, and employees, or to assist the Contractor in the defense. This section does not require the Contractor 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.
- 2.7** During the term of this Agreement, the Contractor will obtain and maintain in force insurance coverage of the types and with the limits as follows:
1. Commercial General Liability Insurance:
The Contractor will maintain occurrence based commercial general liability insurance or equivalent form with a limit of not less than \$1 million for each occurrence. If such insurance contains a general aggregate limit it will apply separately to this Agreement or be no less than two times the occurrence limit. The insurance policy will 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.
 2. Professional Liability Insurance or Miscellaneous Professional Liability Insurance:
The Contractor will procure and maintain professional liability insurance or miscellaneous professional liability insurance with a limit not less than \$1 million.
 3. Business Automobile Liability Insurance:
The Contractor will maintain business automobile liability insurance or equivalent form with a limit of not less than \$1 million for each accident. Such insurance will include coverage for owned, hired, and non-owned vehicles.

4. Workers' Compensation Insurance:

The Contractor will procure and maintain workers' compensation and employers' liability insurance as required by South Dakota or federal law.

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

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

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

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

2.10 This Agreement may be terminated by either party hereto upon thirty (30) days written notice. In the event 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 a breach is affected 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 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 after the State terminates for a breach by Contractor it is determined that Contractor was not at fault, then 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 upon five (5) business days' written notice. The Contractor 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 the Contractor waives any claim against the same.

2.12 This Agreement may not be assigned without the express prior written consent of the State. This Agreement may not be amended except in writing, which writing will be

expressly identified as a part of this Agreement and be signed by an authorized representative of each of the parties to this Agreement.

- 2.13** This Agreement will be governed by and construed in accordance with the laws of the State of South Dakota, 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 will be in Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota.
- 2.14** The Contractor will comply with all federal, tribal, state, and local laws, regulations, ordinances, guidelines, permits, requirements, and other standards applicable to providing services pursuant to this Agreement and will be solely responsible for obtaining current information on such requirements. Nothing herein will constitute a waiver by the State to any defense to jurisdiction nor will anything under this Agreement constitute an acknowledgement by the State that any tribe has or exercises any jurisdiction over this Agreement or the parties.
- 2.15** The Contractor may not use subcontractors to perform the services described in this Agreement without the express prior written consent of the State. The Contractor will include provisions in its subcontracts requiring its subcontractors to comply with the applicable provisions of this Agreement, to indemnify the State, and to provide insurance coverage for the benefit of the State in a manner consistent with this Agreement. The Contractor will cause its subcontractors, agents, and employees to comply with applicable federal, 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 subcontractors. The Contractor will assist in the vetting process.
- 2.16** 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.
- 2.17** The Contractor hereby acknowledges and agrees that all reports, plans, specifications, technical data, miscellaneous drawings, software system programs and documentation, procedures, or files, operating instructions and procedures, source code(s) and documentation, including those necessary to upgrade and maintain the software program, and all information contained therein provided to the State by the Contractor in connection with its performance of services under this Agreement will belong to and is the property of the State and will not be used in any way by the Contractor without the written consent of the State. Papers, reports, forms, software programs, source code(s), and other material which are a part of the work under this Agreement will not be copyrighted without written approval of the State.
- 2.18** The Contractor certifies that neither Contractor nor its principals are presently debarred, suspended, proposed for debarment or suspension, or declared ineligible from participating in transactions by the federal government or any state or local government department or agency. Contractor further agrees that it will immediately notify the State if during the term of this Agreement Contractor or its principals become subject to debarment, suspension, or ineligibility from participating in transactions by the federal government, or by any state or local government department or agency.

2.19 By signing this Agreement, the Contractor certifies and agrees that it has not refused to transact business activities, have not terminated business activities, and have not taken other similar actions intended to limit its commercial relations, related to the subject matter of this Agreement, with a person or entity that is either the State of Israel, or a company doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel to do business, or doing business in the State of Israel, with the specific intent to accomplish a boycott or divestment of Israel in a discriminatory manner. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to terminate this Agreement. During the term of this Agreement, if the Contractor no longer complies with this certification, the Contractor agrees to provide immediate written notice to the State and agrees such noncompliance may be grounds for termination of this Agreement.

2.20 Pursuant to South Dakota Codified Law § 5-18A, by entering into this Agreement with the State of South Dakota, the Contractor certifies and warrants that the Contractor is not a prohibited entity, regardless of its principal place of business, that is ultimately owned or controlled, directly or indirectly, by a foreign national, a foreign parent entity, or foreign government from China, Iran, North Korea, Russia, Cuba, or Venezuela, as defined by South Dakota Codified Law § 5-18A.

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

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

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

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

2.24 The waiver by either party of a breach or violation of any provisions of this Agreement will not operate as, or be construed to be, a waiver of any subsequent breach of the same or other provision of this Agreement.

2.25 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.

- 2.26** Neither party will disclose the contents of the Agreement except as required by applicable law or as necessary to carry out the terms of the Agreement or to enforce that party's rights under this Agreement. The Contractor acknowledges that the State of South Dakota and its agencies are public entities and thus are bound by South Dakota open meetings and open records laws. It is therefore not a breach of this Agreement for the State to take any action that the State reasonably believes is necessary to comply with the South Dakota open records or open meetings laws, including, without limitation, posting this Agreement on the website pursuant to SDCL § 1-27-46.

3 Scope of Work

- 3.1** Conduct a performance review audit of the medical claims process performed by Wellmark for the following three (3) audit periods

Audit Period 1 will be July 1, 2027 to June 30, 2028 (Fiscal Year 2028)

Audit Period 2 will be July 1, 2028 to June 30, 2029 (Fiscal Year 2029)

Audit Period 3 will be July 1, 2029 to June 30, 2030 (Fiscal Year 2030)

- 3.2** Electronic Screening of 100% of paid medical claims paid for each audit period.

- 3.3** For each audit period the electronic screening of 100% of paid medical claims must measure:

1. Claims processing accuracy rate (the incidence of claims processed without errors);
2. Payment incidence accuracy rate (the incidence of claims processed without payment error);
3. Financial accuracy rate (the percentage of paid dollars processed without error);
4. Claims turnaround time (the percentage of claims processed within fourteen (14) and thirty (30) calendar days; and
5. Identification of recovery/savings potential.

- 3.4** The results of the review must be compared to acceptable industry standards and to other similar reviews that the vendor has performed. In addition, the results will be compared to Wellmark's self-reported performance results to assess the reliability of such.

Audit Period 1 Review of a **combined financial stratified/attribute** statistical sample of 200 processed during fiscal year period July 1, 2027, to June 30, 2028. A significant percentage of the sample must be high dollar claims.

Audit Period 2 Review of a **combined financial stratified/attribute** statistical sample of 200 total claims processed during the fiscal year period July 1, 2028, to June 30, 2029. A significant percentage of the sample must be high dollar claims.

Audit Period 3 Review of a **combined financial stratified/attribute** statistical sample of 200 total claims processed during the fiscal year period July 1, 2029, to June 30, 2030. A significant percentage of the sample must be high dollar claims.

3.5 Judgment Claims Reviews Diagnosis-Related Group ("DRG") Hospital Claims

review of a randomly selected judgment sample of fifty (50) inpatient DRG hospital claims for *each Audit Period* will be performed to verify the accuracy of DRG claim processing.

Audit Period 1 Claims will be randomly selected from DRG contracted hospital claims processed during fiscal year period of July 1, 2027, to June 30, 2028 (FY28).

Audit Period 2 Claims will be randomly selected from DRG contracted hospital claims processed during the fiscal year period of July 1, 2028, to June 30, 2029 (FY29).

Audit Period 3 Claims will be randomly selected from DRG contracted hospital claims processed during the fiscal year period of July 1, 2029, to June 30, 2030 (FY 2029).

It is the State's expectation that the audit firm will apply their own logic in identifying which DRGs are most likely to have questionable coding.

3.6 The Vendor will review Out-of-Network Claims for each Audit Period. Claims must be evaluated to verify that payments are consistent with the Wellmark's contractual requirements. In addition to verifying compliance with the Health Plan requirements and any external network arrangements that may apply, a review of the following must be conducted:

1. If claim is subject to an external provider network, such as PHCS (Private Healthcare Systems), which provides supplemental PPO network access, a copy of repricing data from external network, a copy of network contract between vendor and Wellmark, and a copy of the applicable provider contract between the network and specific provider will be required;
2. Detailed reports of claim charges for funding requests from the State Health Plan's bank account; and
3. Wellmark's claim system's payment history records for the plan member.

Audit Period 1 Claims of a randomly selected sample of 20 Out-of-Network ("OON") claims processed during fiscal year time period of July 1, 2027, to June 30, 2028 (FY28).

Audit Period 2 Claims of a randomly selected sample of 20 OON claims processed during fiscal year time period of July 1, 2028, to June 30, 2029 (FY29)

Audit Period 3 Claims of a randomly selected sample of 20 OON claims processed during fiscal year time period of July 1, 2029, to June 30, 2030 (FY30)

3.7 The Contractor must follow HIPAA guidelines and be willing to sign a Business Associate Agreement with the State which is attached as **Exhibit A** – BHRA Business Associate Agreement.

4 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 is under no obligation to solicit such information if it is not included in the proposal. The offeror's failure to submit such information may have an adverse impact on the evaluation of the proposal and may result in the proposal being excluded as non-responsive.
- 4.2** Offeror's Contacts: Offerors and their agents (including subcontractors, employees, consultants, or anyone else acting on their behalf) must direct all their questions or comments regarding the RFP, the evaluation, etc. to the Primary Contact listed on the first page of this RFP. Offerors and their agents may not contact any state employee other than the Primary Contact regarding any of these matters during the solicitation and evaluation process. Inappropriate contacts are ground for suspension and exclusion from specific procurements. Offerors and their agents who have questions regarding this matter should contact the Primary Contact.
- 4.3** The offeror may be required to submit a copy of their most recent audited financial statements upon the State's request.
- 4.4** The offeror must provide the information listed below for at least three contracts, either previous or current, performed by the offeror's organization. The offeror must provide the following information related to at least three previous and current contracts, performed by the offeror's organization, which are like the requirements of this RFP. The offeror must also provide this same information for any of its contracts that have terminated, expired, or not been renewed within the past three years.
- Name, address and telephone number of client and a representative of that agency who may be contracted for verification of all information submitted;
 - Dates of the contract; and
 - A brief, written description of the specific prior services performed and requirements thereof.
- 4.5** No Broker Submission: For the purposes of this RFP, the State will not accept proposals from brokers on behalf of service providers that they represent. The State will receive proposals directly from service providers only. In addition, costs proposed for services cannot include fees, commissions, or revenue sharing (e.g. percentage of discount savings, etc.) with any broker or consultant.

5 Proposal Response Format

- 5.1** The offer must provide one (1) copy of their entire proposal, including all attachments, in Microsoft Word, Excel or PDF electronic format by email to Peggy.Canter@state.sd.us.
- 5.2** The proposal should be page numbered and should have an index and/or a table of contents referring to the appropriate page number.
- 5.3** **Use of State Seal Restriction** The offeror's proposal should refrain from using the State of South Dakota State Seal in its proposal. Offerors are cautioned that use of the State Seal in any of its documents is illegal as per South Dakota Codified Law § 1-6-3.1. *Use of seal or facsimile without authorization prohibited--Violation as misdemeanor. No person may reproduce, duplicate, or otherwise use the official seal of the State of South Dakota,*

or its facsimile, adopted and described in §§ 1-6-1 and 1-6-2 for any for-profit, commercial purpose without specific authorization from the secretary of state. A violation of this section is a Class 1 misdemeanor.

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

5.4.1 RFP Form. The State's Request for Proposal form (see page 1 of this RFP) completed and signed.

5.4.2 Executive Summary. The one (1) or two (2) page executive summary is to briefly describe the offeror's proposal. The summary should highlight the major features of the proposal. It must indicate any requirements, including any of the technical or cyber security 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.

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

- a. 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.
- b. A specific point-by-point response, in the order listed to each requirement described in Section 3.0: Scope of Work and Section 4.0: Proposal Requirements and Company Qualifications of the RFP. The response should identify each requirement being addressed as enumerated in the RFP.
- c. A clear description of any options or alternatives proposed.

5.5 Response to State's IT Terms The offeror's proposal must highlight any requirement in Section 4 that the offeror's proposed deliverables cannot comply with, and the offeror must provide any suggested "work-around" to the requirement in question or a future date that the offeror will be able to comply with the requirement.

5.6 Response to State's Standard Contract Terms: The offeror's proposal must indicate any issues the offeror has with specific contract terms found in Section 2 and Exhibit B. If the offeror does not indicate that there is an issue with a specific contract term, then the offeror will be deemed to have accepted the contract terms as written.

6 Proposal Evaluation and Award Process

6.1 After determining that a proposal satisfies the minimum requirements stated in the Request for Proposal, the evaluator(s) will use subjective judgment in conducting a

comparative assessment of the proposal by considering each of the following criteria, on a 1,000-point scale.

Description	Points
Specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements	200
Resources available to perform the work, including any specialized services, within the specified time limits for the project	175
Record of past performance, including price and cost data from previous projects, quality of work, ability to meet schedules, cost control, and contract administration	175
Availability to the project locale	50
Familiarity with the project locale	50
Proposed project management techniques	50
Ability and proven history in handling special project constraints	100
Cost	200

- 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 the best interest of the State.
- 6.5** Award: BHRA and the highest ranked offeror will mutually discuss and refine the scope of services for the project and will negotiate terms, including compensation and performance schedule.
- 6.5.1** If BHRA 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 State, BHRA will, either orally or in writing, terminate negotiations with the offeror. BHRA may then negotiate with the next highest ranked offeror.
- 6.5.2** The negotiation process may continue through successive offerors, according to BHRA ranking, until an agreement is reached or BHRA terminates the

contracting process.

7 Cost Proposal

- 7.1** Cost Proposal must detail cost breakdown for all audit services. The cost proposal shall include all direct and indirect expenses.
- 7.2** Cost Proposal must break out cost related to subject matter expert(s) professional services team, conference call time and travel expenses.

8 GENERAL IT REQUIREMENTS

If an offeror's proposal includes an IT aspect, such as a web portal for data sharing or report deliver, the following applies:

8.1 Artificial Intelligence Use

The offeror must provide an explanation of its use of Artificial Intelligence, both in its proposed solution and the development lifecycle of the proposed solution. This requirement includes the offeror's use of Generative AI (GenAI) tools/products. For GenAI tools/products, the offeror must provide the following:

- GenAI model name,
- product owner,
- product description (including purpose, functionality, and key characteristics),
- use case (or goal e.g. image recognition, natural language processing, text summarization),
- the intended information use (context for how information is used in the model) for the GenAI included in the offeror's proposal,
- the geographical location of the tool, and
- how the offeror monitors and audits the tool's compliance on use restrictions, data restrictions, legal compliance (non-discriminatory outputs), and biases in the tool's outputs.

8.2 Hosting and Data Access Requirements

The State will own all data tables created as a result of the Agreement. The State must have the ability 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.

The offeror's proposal must describe how the State can access data housed within the proposed solution for ingestion into a state data repository, encompassing available methodologies (e.g., application programming interface (API), flat file), data formatting, frequency of updates, and any inherent constraints. Additionally, the offeror's proposal must provide a high-level architecture diagram, as part of the solution diagram, explaining the proposed solution's data provision mechanism.

If available, the offeror must provide separate, complete proposals for the offeror's proposed solution to be hosted by the offeror, by the State on its internal infrastructure, and on the State's Azure cloud hosted tenant as a PaaS solution. If any of the hosting

options is not available, the offeror must clearly state that in the offeror's proposal and provide an explanation as to why the hosting option is not available.

8.3 Single Sign-On Requirements

If the offeror's proposal includes a deliverable with a login component, the proposal must describe how the deliverable will integrate with the State's standard identity management service single sign-on (SSO).

The State's 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. The State's SSO requirement and links to Microsoft's official documentation can be found at: https://www.sd.gov/bit?id=bit_standards_single_sign_on

If the offeror cannot fulfill this identity management standard, the offeror's proposal will be rejected from consideration.

8.4 SSO Logout Initiation Requirements

- The offeror's deliverable must provide users with a clear and easily accessible logout mechanism (e.g., a "Logout" button/link).
- The logout functionality of the offeror's deliverable must trigger a session-based logout process utilizing the sign-out endpoint found in the metadata document provided during implementation.

8.5 Session Timeout Requirements

- The offeror's deliverables must allow for a customizable, State-defined inactive user session timeout period.
- The offeror's deliverables must notify users of impending session expiration five minutes before the timeout occurs, providing users with the option to extend the session.

8.6 Session Termination on Browser Close Requirement

The offeror's deliverables must clearly notify users that closing the browser window or tab is not a valid logout because the SSO session may remain active. The notice must further notify users that they are responsible for explicitly logging out to ensure complete session termination.

8.7 Onboarding/Provisioning of Users Requirement

The offeror's proposal must describe how new users are onboarded or provisioned into the deliverable. The offeror must provide an automated process for onboarding and offboarding users or must provide a process that requires minimal manual steps.

8.8 Interfaces and Integration Requirements

The offeror's proposal must describe how the deliverables can adapt to business

necessary interfaces using widely adopted open APIs and standards. Additionally, the offeror must make available or expose software services that would enable third-party developers to interface other business applications. The offeror must publish documentation for the software services in question. The offeror's proposal must include a detailed description of system capability.

8.9 Web Application Vulnerability Scan Requirements

Any web-based deliverable must undergo a web application vulnerability scan ("Vulnerability Scan"). The Vulnerability Scan must identify misconfigurations or vulnerabilities such as those found in the OWASP Top Ten and must detail the certainty level of each finding.

Unless expressly indicated in writing, the State assumes all price estimates and bids are for the delivery and support of deliverables that will pass Vulnerability Scans. If the State determines that any aspect of the deliverable has 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 deliverable does not pass the initial Vulnerability Scan or the offeror cannot provide a satisfactory Vulnerability Scan report, additional scans may be required to confirm the deliverable is secure.

8.9.1 State Hosted: For state hosted web-based deliverables, the Vulnerability Scan will be performed by the State and the offeror's proposal should take that into consideration when responding to this RFP. As a condition of the resulting contract, the state hosted web-based deliverable will have to successfully pass the Vulnerability Scan prior to the deliverable being allowed to go in a production environment. Any offeror who responds to this RFP must accept such a contract term and must factor this security requirement into the offeror's proposal.

8.9.2 Vendor Hosted: For vendor hosted web-based deliverables, any offeror who makes it to the "Tech Review" stage of the RFP process must provide the State a copy of the full report of the deliverable's most recent Vulnerability Scan, a summary will not be accepted. The offeror should mark the vulnerability report as "Confidential" if it treats such a report as confidential information. If the offeror requires a Non-Disclosure Agreement (NDA) to be in place before the State may review the Vulnerability Scan report, the offeror must notify the State of such a requirement and resolve the signing of an NDA with enough time to respond to this RFP within the timeframe.

The offeror's Vulnerability Scan report must consist of, at a minimum:

- The system that was evaluated,
- The categories that were evaluated (examples: SQLi, XSS, or RCE),
- What were the general findings,
- Technical detail of each issue found,
- Remediation status of enumerated issues (if any).

The cost of any Vulnerability Scans done by the offeror or the offeror's costs

associated with the State performing Vulnerability Scans must be part of the offeror's cost proposal. Failure of a deliverable to satisfactorily pass a Vulnerability Scan may result in the offeror's proposal being rejected.

8.10 Banned Entity Requirement

The offeror's proposed deliverables 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 of America under the International Emergency Economic Powers Act, in a United States appropriation bill, an Executive Order, or listed on the US Department of Commerce's Entity List will be included in this ban.

8.11 Access Management Requirement

If the offeror's proposed deliverables require 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 proposal. All costs associated with providing an account to the offeror will be borne by the agency.

8.12 Web Content Accessibility Guidelines Requirement

The offeror's proposed deliverables must conform to the Web Content Accessibility Guidelines 2.1 Level AA.

8.13 Browser Compatibility

The offeror's proposed deliverables must be compatible with supported versions of Edge, Chrome, Safari, and Firefox browsers.

9 VENDOR HOSTED SOLUTION REQUIREMENTS

9.1 General Vendor Hosted Requirements

In the offeror's proposal, the offeror must describe its:

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

9.2 Import and Export of Data Requirement

The offeror's proposed deliverables must allow the State the ability to import or export the State's data piecemeal or in its entirety at the State's discretion without interference from the offeror. The data must be able to be exported in a non-proprietary format and must include information such as metadata (data structure descriptions, data dictionary, and data). The offeror's proposal must describe how this functionality works within its deliverables.

10 RESOURCES

10.1 Staff Resumes and References

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

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

11 Corporate Qualifications

11.1 Offeror Company Information

The offeror's proposal must include responses to each of the following questions:

- What year was your firm established?
- What is your firm's website?

- Has your firm ever done business under a different name and if so, what was the name?
- How many employees does your firm have?
- How many employees in your firm are involved in this type of project?
- How many of those employees are involved in on-site project work?
- Has your firm ever done business with other governmental agencies? If so, please provide references.
- Has your firm ever done business with the State of South Dakota? If so, please provide references.
- Has your firm ever done projects that are exactly like or similar to this project?
- How many clients are currently using your proposed solution? How many of those clients are public sector: local, state, and federal?

11.2 Offeror Parent Company

If the offeror has a parent company, the offeror's proposal must include responses to the following questions:

- What is the name of your parent company?
- What year was your parent company established?
- What is your parent company's website?
- What is the business of your parent company?
- What is the total number of employees in the parent company?
- What are the total revenues of your parent company?
- How many employees of your parent company have the skill set to support this effort?
- How many of those employees are accessible to your organization for active support?
- What percent of your parent company's revenue (if applicable), is produced by your firm?

11.3 Team Organization and Staff Resumes

11.4 Background Investigations

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 or federal statute as confidential or have access to secure facilities will have fingerprint-based background investigations. These background investigations 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 subcontractors, agents, assigns, and affiliated entities.

12 Best and Final Offers

The State reserves the right to request best and final offers; best and final offers cannot be initiated by an offeror. Best and final offers may not be necessary if the State is satisfied with the proposals received.

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

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

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

In the event of any inconsistency or conflict between the terms of this Exhibit and the terms of the main body of the Agreement or any other exhibit or attachment to the Agreement, the terms of this Exhibit will take precedence.

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 \$[cyber_insurance_amount] 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. 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 V. Non-Disclosure and Separation of Duties

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

Section VI. 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 VII. 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 VIII. 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 IX. 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 X. 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 XI. 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 XII. 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 XIII. 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 XIV. 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 with 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 XV. 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 XVI. 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 XVII. Security

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

By signing this Agreement, the Vendor warrants that:

- A. All Critical, High, Medium, and Low security issues are resolved. Critical, High, Medium, and Low can be described as follows:
 - 1. **Critical** - Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices.
 - 2. **High** - The vulnerability is difficult to exploit; however, it is possible for an expert in Information Technology. Exploitation could result in elevated privileges.
 - 3. **Medium** - Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. Denial of service vulnerabilities that are difficult to set up.
 - 4. **Low** - Vulnerabilities identified by the State as needing to be resolved that are not Critical, High, or Medium issues.
- B. Assistance will be provided to the State by the Vendor in performing an investigation to determine the nature of any security issues that are discovered or are reasonably suspected after acceptance. The Vendor will fix or mitigate the risk based on the following schedule: Critical and high risk, within 7 days, medium risk within 14 days, low risk, within 30 days.

Section XVIII. 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 XIX. 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 XX. Web and Mobile Applications

The Vendor's application is required to:

- A. 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,
- B. encrypt data in transport and at rest using a mutually agreed upon encryption format,
- C. close all connections and close the application at the end of processing,
- D. 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,
- E. have no code not required for the functioning of application,
- F. 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,
- G. 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,
- H. have no connections to any service not required by the functional requirements of the application or defined in the project requirements documentation,
- I. 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),
- J. 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,
- K. access no data outside what is defined in the "About" information for the Vendor's application,
- L. conform to Web Content Accessibility Guidelines 2.1 Level AA, and
- M. any application to be used on a mobile device must be password protected.

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 XXI. Integration with State's Single Sign-On

Any software or application provided to, or being paid for by, the State pursuant to this Agreement must integrate with the State's standard identity management service single sign-on ("SSO"). The current State standard protocols used for SSO are OpenID Connect and OAuth 2.0, the latter being the preferred protocol. No software, application, or Agreement deliverable will be deemed accepted until the requirements of this Section have been satisfied.

The Vendor agrees that the total cost of the Agreement has incorporated the necessary time and expense of integrating the software or application deliverables with the State's SSO. The State will

not pay any additional money for SSO integration beyond what is agreed to in the total cost of the Agreement. The Parties agree the State may withhold any final payment for a specific software or application deliverable until the SSO integration is complete and acceptance has occurred.

Section XXII. 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 XXIII. 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 XXIV. 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. The only exceptions are when the State Data must be maintained after the project is completed for legal reasons or the State Data is on a backup medium where the State Data cannot be separated from other data. If the State Data cannot be sanitized for these reasons, then the Vendor must encrypt the data to at least 256 AES with SHA 2 or SHA 256 hashing and maintain the medium in a facility that meets the security requirements of the most current version of NIST 800-53 or IRS 1075 whichever is relevant.

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 XXV. 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 XXVI. 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 XXVII. 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 XXVIII. 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 XXIX. 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 XXX. 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 XXXI. 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 XXXII. Security Scan Report

The Vendor will provide the State, at no cost to the State, and at a date and time and for the duration agreeable to both parties, a security scan report of the Vendor's system and data. The security scan report will include mutually agreed to information. The security scan report must show an acceptable security, as defined by the State. At the Vendor's sole expense, the Vendor will work with the State to rectify any Critical and High security defects indicated by the security scan prior to the State engaging the Vendor. After rectifying the security defects, the Vendor will provide the State a scan that demonstrates that the security defects were rectified, to the State's satisfaction, at no additional cost to the State. The State may collaborate, at the State's discretion, with the Vendor on remediation efforts. These remediation efforts will not be considered a violation of any licensure agreements between the State and the Vendor. The State will not be charged for any costs incurred by the Vendor in these remediation efforts unless agreed to by the State in advance and in writing. Security defects are defined to be:

- A. **Critical** – Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices.
- B. **High** – The vulnerability is difficult to exploit; however, it is possible for an expert in Information Technology. Exploitation could result in elevated privileges.

Section XXXIII. 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 XXXIV. 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 XXXV. 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.