

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

Division of Medical Services Health Home Recipient Monthly Attribution

PROPOSALS ARE DUE NO LATER THAN APRIL 3, 2024 5:00 PM CST

RFP10472

BUYER:
Division of Medical Services

POC: Kirsten Blachford
Kirsten.Blachford@state.sd.us

READ CAREFULLY

FIRM NAME: _____ AUTHORIZED SIGNATURE: _____
(Digital Signature allowed)

ADDRESS: _____ TYPE OR PRINT NAME: _____

CITY/STATE: _____ TELEPHONE NO: _____

ZIP (9 DIGIT): _____ FAX NO: _____

FEDERAL TAX ID#: _____ E-MAIL: _____

PRIMARY CONTACT INFORMATION

CONTACT NAME: _____ TELEPHONE NO: _____

FAX NO: _____ E-MAIL: _____

1.0 GENERAL INFORMATION

1.1 **PURPOSE OF REQUEST FOR PROPOSAL (RFP)**

The purpose of this RFP is to select a vendor to conduct a monthly review of claims and then deem Medicaid recipients eligible for the Health Home Program. The vendor will also determine the Tier and continuity of Care provider of the recipients using the CDPS system. The vendor will provide a monthly file to DSS with the results.

DSS requires other reports as outlined in the SCOPE in section 3.0.

1.2 **ISSUING OFFICE AND RFP REFERENCE NUMBER**

The Division of Medical Services is the issuing office for this document and all subsequent addenda relating to it, on behalf of the State of South Dakota, Department of Social Services. The reference number for the transaction is RFP10472. Refer to this number on all proposals, correspondence, and documentation relating to the RFP.

Please refer to the Department of Social Services website link <http://dss.sd.gov/keyresources/rfp.aspx> for the RFP, any related questions/answers, changes to schedule of activities, amendments, etc.

1.3 **SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)**

RFP Publication	March 6, 2024
Offeror Questions	March 20, 2024
Responses to Offeror Questions	March 27, 2024
Request for SFTP Folder	April 2, 2024
Proposal Submission	April 3, 2024
Site visits Scheduled as needed	April 22-26, 2024
Anticipated Award Decision/Contract Negotiation	April 30, 2024

1.4 **SUBMITTING YOUR PROPOSAL**

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

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

Proposals maybe submitted as PDFs via Secured File Transfer Protocol (SFTP). Offerors must request an SFTP folder no later than April 3, 2024 by 5 PM CST, by emailing Kirsten Blachford at the email indicated on page one. The subject line must be **RFP10472 SFTP Request**. The email should contain the name and the email of the person who will be responsible for uploaded the document(s).

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

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

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

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

1.6 NON-DISCRIMINATION STATEMENT

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

1.7 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 an entity, regardless of its principal place of business, that is ultimately owned or controlled, directly or indirectly, by a foreign national, a foreign parent entity, or foreign government from China, Iran, North Korea, Russia, Cuba, or Venezuela, as defined by South Dakota Executive Order 2023-02. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to reject the bid or response submitted by the bidder or offeror on this project and terminate any contract awarded based on the bid or response. The successful bidder or offeror further agrees to provide immediate written notice to the contracting executive branch agency if during the term of the contract it no longer complies with this certification and agrees such noncompliance may be grounds for contract termination.

1.9 CERTIFICATION OF NO STATE LEGISLATOR INTEREST

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

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

1.10 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.

1.11 OFFEROR INQUIRIES

Offerors may email inquiries concerning this RFP to obtain clarification of requirements. No inquiries will be accepted after March 20, 2024. Email inquiries must be sent to Kirsten.Blachford@state.sd.us with the following wording, exactly as written, in the subject line: **RFP10472 Questions**.

The Department of Social Services (DSS) will respond to offerors' inquiries by posting offeror aggregated questions and Department responses on the DSS website at <http://dss.sd.gov/keyresources/rfp.aspx> no later than March 27, 2024. For expediency, DSS may combine similar questions. Offerors may not rely on any other statements, either of a written or oral nature, that alter any specification or other term or condition of this RFP. Offerors will be notified in the same manner as indicated above regarding any modifications to this RFP.

1.12 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.

Offerors may submit a redacted copy of their proposal when they respond though this is optional.

1.13 LENGTH OF CONTRACT

The proposed contract would begin on June 1, 2024 and go through May 31, 2027 with the option to renew for 2 -1 year periods.

1.14 GOVERNING LAW

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

1.15 DISCUSSIONS WITH OFFERORS (ORAL PRESENTATION/NEGOTIATIONS)

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

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

2.0 STANDARD AGREEMENT TERMS AND CONDITIONS

Any contract or agreement resulting from this RFP will include, at minimum, the State's standard terms and conditions as seen in **Attachment A**. The Business Associate Agreement (BAA) is added as **Attachment B**.

The Bureau of Information and Telecommunications (BIT) Required State Hosted IT Contract Terms are included as **Attachment C** and required security and vendor questions are included as **Attachment D**.

The offeror should indicate in their response any issues they have with any specific contract terms. If the offeror does not indicate any contract term issues, then the State will assume the terms are acceptable.

3.0 SCOPE OF WORK

DSS is seeking a qualified individual to perform the monthly Health Home attribution process. Activities include but are not limited to:

- 3.1 Determination of members who are eligible for the Health Home program – Using the list of ICD-10 codes provided by the state, review the 15 months' worth of claims files and determine which recipients qualify for the Health Home Program. File layout will be provided upon request.
 - 3.1.1 Medicaid recipients with two or more chronic conditions or recipients with one chronic condition who are at risk for a second chronic condition. Chronic conditions include: Mental Health Condition, Substance Use Disorder Asthma, COPD, Diabetes, Heart Disease, Hypertension, Obesity, Musculoskeletal and Neck/Back disorders. At-risk conditions include: Pre-Diabetes, tobacco use, Cancer, Hypercholesterolemia, Depression, and use of multiple medications (6 or more classes of drugs); or
 - 3.1.2 Recipients who have a Severe Mental Illness or Emotional Disturbance.
- 3.2 Assign eligible members to Health Home Tiers 1-4 using the Chronic Illness and Disability Payment System.
- 3.3 Utilizing the State's SFTP service, return results to the state monthly basis on the agreed upon date and format. The File layout and format will be provided upon request. Data files returned will also include a list of individuals whose Tier was listed as 1 due to the requirement to move recipients currently in an LTC facility to a Tier 1. The Report should include the recipient ID and the recipient's real tier prior to the movement to a Tier 1.
- 3.4 Determination of eligible members to continuity of care provider. Use the claims data provided to find the continuity of care provider using the algorithm outlined by the state.
- 3.5 Vendors should outline when they can deliver the first set of files. Priority will be given to the vendors who can deliver the first files by no later than Mid July.
- 3.6 Utilizing the State's SFTP service, provide a yearly demographics reports defined by DSS. File Format and layout available upon request.
- 3.7 Utilizing the State's SFTP service, provide an update tier file annually for January 1 re-tiering as defined by DSS. File Layout and format available upon request.
- 3.8 Have the systems and software infrastructure necessary to support these tasks. Please provide your process for securely storing and providing the State's Data.

4.0 PROPOSAL REQUIREMENTS AND COMPANY QUALIFICATIONS

- 4.1 Vendor should have the following qualifications:

- 4.1.1 Multiple years (3 or more) of working with Medicaid Claims data.
- 4.1.2 Multiple years (3 or more) using CDPS to establish the Tier of recipients for a Medicaid Health Home Program.
- 4.2 Provide the following information related to at least three previous and current service/contracts performed by the offeror's organization which are similar to the requirements of this RFP. Provide this information as well for any service/contract that has been terminated, expired or not renewed in the past three years:
 - a. Name, address and telephone number of client/contracting agency and a representative of that agency who may be contacted for verification of all information submitted;
 - b. Dates of the service/contract; and
 - c. A brief, written description of the specific prior services performed and requirements thereof.
- 4.3 The offeror must submit information that demonstrates their availability and familiarity with the locale in which the project (s) are to be implemented.
- 4.4 The offeror must describe their proposed project management techniques.
- 4.5 The offeror is cautioned that it is the offeror's sole responsibility to submit information related to the evaluation categories and that the State of South Dakota is under no obligation to solicit such information if it is not included with the proposal. The offeror's failure to submit such information may cause an adverse impact on the evaluation of the proposal.
- 4.6 **Offeror's Contacts:** Offerors and their agents (including subcontractors, employees, consultants, or anyone else acting on their behalf) must direct all of their questions or comments regarding the RFP, the evaluation, etc. to the buyer of record indicated on the first page of this RFP. Offerors and their agents may not contact any state employee other than the buyer of record regarding any of these matters during the solicitation and evaluation process. Inappropriate contacts are grounds for suspension and/or exclusion from specific procurements. Offerors and their agents who have questions regarding this matter should contact the buyer of record.
- 4.7 If an offeror's proposal is not accepted by the State, the proposal will not be reviewed/evaluated.
 - 4.7.1 Not received on time.
 - 4.7.2 Not signed by the offeror.

5.0 PROPOSAL RESPONSE FORMAT

- 5.1 Only a PDF copy shall be submitted.
 - 5.1.1 As outlined in section 1.4 "SUBMITTING YOUR PROPOSAL" proposals shall only be submitted electronically via SFTP.
 - 5.1.2 The proposal should be page numbered and should have an index and/or a table of contents referencing the appropriate page number.
- 5.2 Proposals submitted electronically should contain the following:
 - 5.2.1 **RFP Form.** The State's Request for Proposal form completed and signed.
 - 5.2.2 **Executive Summary.** The one or two page executive summary is to briefly describe the offeror's proposal. This summary should highlight the major features of the proposal. It must indicate any requirements that cannot be met by the offeror. The reader should be able to determine the essence of the proposal by reading the executive summary. Proprietary information requests should be identified in this section.

- 5.2.3 **Detailed Response.** This section should constitute the major portion of the proposal and must contain at least the following information:
- 5.2.3.1 A complete narrative of the offeror's assessment of the work to be performed, the offeror's ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the offeror's understanding of the desired overall performance expectations.
 - 5.2.3.2 A specific point-by-point response, in the order listed, to each requirement in the RFP as detailed in Sections 3 and 4. The response should identify each requirement being addressed as enumerated in the RFP.
 - 5.2.3.3 A clear description of any options or alternatives proposed.
- 5.2.4 **Cost Proposal.** Cost will be evaluated independently from the technical proposal. Offerors may submit multiple cost proposals. All costs related to the provision of the required services must be included in each cost proposal offered.
- See section 7.0 for more information related to the cost proposal.
- 5.2.5 The Bureau of Information and Telecommunications (BIT) required security and vendor questions are included as **Attachment D**. This will need to be completed and returned with offerors proposal.

6.0 PROPOSAL EVALUATION AND AWARD PROCESS

- 6.1 After determining that a proposal satisfies the mandatory requirements stated in the Request for Proposal, the evaluator(s) shall use subjective judgment in conducting a comparative assessment of the proposal by considering each of the following criteria listed in order of importance:
- 6.1.1 Specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements;
 - 6.1.2 Resources available to perform the work, including any specialized services, within the specified time limits for the project;
 - 6.1.3 Record of past performance, including price and cost data from previous projects, quality of work, ability to meet schedules, cost control, and contract administration;
 - 6.1.4 Availability to the project locale;
 - 6.1.5 Familiarity with the project locale;
 - 6.1.6 Proposed project management techniques;
 - 6.1.7 Ability and proven history in handling special project constraints, and
 - 6.1.8 Cost proposal.
- 6.2 Experience and reliability of the offeror's organization are considered subjectively in the evaluation process. Therefore, the offeror is advised to submit any information which documents successful and reliable experience in past performances, especially those performances related to the requirements of this RFP.
- 6.3 The qualifications of the personnel proposed by the offeror to perform the requirements of this RFP, whether from the offeror's organization or from a proposed subcontractor, will be subjectively

evaluated. Therefore, the offeror should submit detailed information related to the experience and qualifications, including education and training, of proposed personnel.

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

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

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

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

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

7.0 COST PROPOSAL

7.1 The Offeror should include the following in a Cost proposal:

7.1.1 Cost of providing the defined service by year for the first three years.

7.1.2 Cost of providing the defined service for year 4 and 5.

7.1.3 Frequency of Billing.

ATTACHMENT A

**STATE OF SOUTH DAKOTA
DEPARTMENT OF SOCIAL SERVICES
DIVISION OF MEDICAL SERVICES**

**Consultant Contract
For Consultant Services
Between**

State of South Dakota
Department of Social Services
DIVISION OF MEDICAL SERVICES
700 Governors Drive
Pierre, SD 57501-2291

Referred to as Consultant

Referred to as State

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

1. CONSULTANT'S South Dakota Vendor Number is . Upon execution of agreement, Consultant will provide the State with Consultant's Employer Identification Number or Federal Tax Identification Number.
2. PERIOD OF PERFORMANCE:
 - A. This Agreement shall be effective as of June 1, 2024 and shall end on May 31, 2027 with the option to renew 2 – 1 year periods, unless sooner terminated pursuant to the terms hereof.
 - B. Agreement is the result of request for proposal process RFP10472.
3. PROVISIONS:
 - A. The Purpose of this Consultant contract is:
 1. To conduct a monthly review of claims then deem Medicaid recipients eligible for the Health Home Program. The vendor will also determine the Tier and continuity of Care provider of the recipients using the CDPS system. The vendor will provide a monthly file to DSS with the results.
 2. Does this Agreement involve Protected Health Information (PHI)? YES (X) NO ()
If PHI is involved, a Business Associate Agreement must be attached and is fully incorporated herein as part of the Agreement (refer to attachment) .
 3. The Consultant WILL () WILL NOT (X) use state equipment, supplies or facilities.
 4. If WILL is indicated above, the following state equipment, supplies, or facilities will be used.
 - B. The Consultant agrees to perform the following services (add an attachment if needed):
 - 1.
 - C. The State agrees to:
 - 1.
 2. Make payment for services upon satisfactory completion of services and receipt of bill. Payment will be in accordance with SDCL 5-26-2.
 3. Will the State pay Consultant expenses as a separate item?

YES () NO (X)

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

D. The TOTAL CONTRACT AMOUNT will not exceed \$ _____ .

4. BILLING:

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

5. TECHNICAL ASSISTANCE:

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

6. LICENSING AND STANDARD COMPLIANCE:

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

7. ASSURANCE REQUIREMENTS:

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

8. COMPLIANCE WITH EXECUTIVE ORDER 2020-01:

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

9. COMPLIANCE WITH SDCL ch 5-18A:

Contractor certifies and agrees that the following information is correct:

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

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

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

10. CERTIFICATION OF NO STATE LEGISLATOR INTEREST:

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

11. RETENTION AND INSPECTION OF RECORDS:

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

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

12. WORK PRODUCT:

Consultant hereby acknowledges and agrees that all reports, plans, specifications, technical data, drawings, software system programs and documentation, procedures, files, operating instructions and procedures, source code(s) and documentation, including those necessary to upgrade and maintain the software program, State Proprietary Information, as defined in the Confidentiality of Information paragraph herein, state data, end user data, Protected Health Information as defined in 45 CFR 160.103, and all information contained therein provided to the State by the Consultant in connection with its performance of service under this Agreement shall belong to and is the property of the State and will not be used in any way by the Consultant without the written consent of the State.

Paper, reports, forms, software programs, source code(s) and other materials which are a part of the work under this Agreement will not be copyrighted without written approval of the State. In the unlikely event that any copyright does not fully belong to the State, the State nonetheless reserves a royalty-free, non-exclusive, and

irrevocable license to reproduce, publish, and otherwise use, and to authorize others to use, any such work for government purposes.

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

13. TERMINATION:

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

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

14. FUNDING:

This Agreement depends upon the continued availability of appropriated funds and expenditure authority from the Legislature for this purpose. If for any reason the Legislature fails to appropriate funds or grant expenditure authority, or funds become unavailable by operation of the law or federal funds reduction, this Agreement will be terminated by the State upon five day written notice. Consultant agrees that termination for any of these reasons is not a default by the State nor does it give rise to a claim against the State or any officer, agent or employee of the State and Consultant waives any claim against the same.

15. ASSIGNMENT AND AMENDMENTS:

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

16. CONTROLLING LAW:

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

17. THIRD PARTY BENEFICIARIES:

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

18. SUPERSESION:

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

19. IT STANDARDS:

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

20. SEVERABILITY:

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

21. NOTICE:

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

22. SUBCONTRACTORS:

The Consultant may not use subcontractors to perform the services described herein without express prior written consent from the State. The State reserves the right to reject any person from the Agreement presenting insufficient skills or inappropriate behavior.

The Consultant 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 Consultant will cause its subcontractors, agents, and employees to comply with applicable federal, state and local laws, regulations, ordinances, guidelines, permits and requirements and will adopt such review and inspection procedures as are necessary to assure such compliance. The State, at its option, may require the vetting of any subcontractors. The Consultant is required to assist in this process as needed.

23. STATE'S RIGHT TO REJECT:

The State reserves the right to reject any person or entity from performing the work or services contemplated by this Agreement, who present insufficient skills or inappropriate behavior, or is considered by the state to be a security risk.

24. INDEMNIFICATION:

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

25. INSURANCE:

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

A. Commercial General Liability Insurance:

Consultant shall maintain occurrence-based commercial general liability insurance or an equivalent form with a limit of not less than \$1,000,000 for each occurrence. If such insurance contains a general aggregate limit, it shall apply separately to this Agreement or be no less than two times the occurrence limit. The insurance policy shall name the State of South Dakota, its officers and employees, as additional insureds, but liability coverage is limited to claims not barred by sovereign immunity. The State of South Dakota, its officers and employees do not hereby waive sovereign immunity for discretionary conduct as provided by law.

B. Professional Liability Insurance or Miscellaneous Professional Liability Insurance:

Consultant agrees to procure and maintain professional liability insurance with a limit not less than \$1,000,000.

C. Business Automobile Liability Insurance:

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

D. Worker's Compensation Insurance:

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

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

26. CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY, AND VOLUNTARY EXCLUSION:

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

27. CONFLICT OF INTEREST:

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

28. CONFIDENTIALITY OF INFORMATION:

For the purpose of the sub-paragraph, "State Proprietary Information" shall include all information disclosed to the Consultant by the State. Consultant acknowledges that it shall have a duty to 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. Consultant shall 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 consultants except those who have agreed to obligations of confidentiality at least as strict as those set out in this Agreement and who have a need to know such information. Consultant 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.

Consultant shall protect confidentiality of the State's information from the time of receipt to the time that such information is either returned to the State or destroyed to the extent that it cannot be recalled or reproduced. State Proprietary Information shall not include information that (i) was in the public domain at the time it was disclosed to Consultant; (ii) was known to Consultant without restriction at the time of disclosure from the State; (iii) that is disclosed with the prior written approval of State's officers or employees having authority to disclose such information; (iv) was independently developed by Consultant without the benefit or influence of the State's information; (v) becomes known to Consultant without restriction from a source not connected to the State of South Dakota. State's Proprietary Information shall include names, social security numbers, employer numbers, addresses and all other data about applicants, employers or other clients to whom the State provides services of any kind. Consultant understands that this information is confidential and protected under applicable State law at SDCL 1-27-1.5, modified by SDCL 1-27-1.6, SDCL 28-1-29, SDCL 28-1-32, and SDCL 28-1-68 as applicable federal regulation and agrees to immediately notify the State if the information is disclosed, either intentionally or inadvertently. The parties mutually agree that neither of them shall disclose the contents of the Agreement except as required by applicable law or as necessary to carry out the terms of the Agreement or to enforce that party's rights under this Agreement. Consultant acknowledges that the State and its agencies are public entities and thus are bound by South Dakota open meetings and open records laws. It is therefore not a breach of this Agreement for the State to take any action that the State reasonably believes is necessary to comply with the South Dakota open records or open meetings laws. If work assignments performed in the course of this Agreement require additional security requirements or clearance, the Consultant will be required to undergo investigation or may be required to sign separate confidentiality agreements, and it will limit access to the confidential information and related work activities to employees that have executed such agreements.

29. REPORTING PROVISION:

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

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

30. DAVIS-BACON ACT:

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

31. COMPLIANCE WITH 40 U.S.C. 3702 AND 3704:

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

32. FUNDING AGREEMENT AND "RIGHTS TO INVENTION":

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

33. FORCE MAJEURE:

Notwithstanding anything in this Agreement to the contrary, neither party shall be liable for any delay or failure to perform under the terms and conditions of this Agreement, if the delay or failure is caused by war, terrorist

attacks, riots, civil commotion, fire, flood, earthquake or any act of God, or any causes beyond the party's reasonable control provided, however that in order to be excused from delay or failure to perform, the party must act diligently to remedy the cause of such delay or failure and must give notice to the other party as provided in this Agreement as soon as reasonably possible of the length and cause of the delay in performance.

33. SOVEREIGN IMMUNITY:

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

34. WAIVER OF BREACH:

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

35. HEADINGS:

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

36. AUTHORITY TO EXECUTE:

Consultant represents and warrants that the execution, delivery, and performance of this Agreement has been duly authorized by Consultant and that no approval, authorization, or consent of any governmental or regulatory agency is required to be obtained in order for Consultant to enter into this Agreement and perform its obligations under this Agreement. If the Consultant is a corporation, said corporation is duly incorporated, validly existing, and in good standing under the laws of its state of incorporation and has all requisite corporate power and authority to execute, deliver, and perform its obligations under this Agreement. If Consultant is an individual person, partnership, or other non-corporate entity, Consultant is authorized to conduct business in and is in good standing in each jurisdiction in which Consultant will conduct business in connection with this Agreement. Consultant has obtained all licenses, certifications, permits, and authorizations necessary to perform the services under this Agreement and currently is in good standing with all regulatory agencies that regulate any or all aspects of Consultant's performance of the services. Consultant will maintain all required certifications, licenses, permits and authorizations during the term of this Agreement at its own expense.

37. AUTHORIZED SIGNATURES:

In witness hereto, the parties signify their agreement by affixing their signatures hereto.

NO SIGNATURE REQUIRED AT THIS TIME

Consultant Signature

Date

Consultant Printed Name

State - DSS Division Director Heather Petermann

Date

State - DSS Chief Financial Officer Jason Simmons

Date

State – DSS Cabinet Secretary Matthew K. Althoff

Date

State Agency Coding:

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

DSS Program Contact Person _____
Phone _____

DSS Fiscal Contact Person _____
Phone Contract Accountant
605 773-3586

Consultant Program Contact Person _____
Phone _____
Consultant Program Email Address _____

Consultant Fiscal Contact Person _____
Phone _____
Consultant Fiscal Email Address _____

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

CERTIFICATION REQUIRED BY SDCL ch 5-18A

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

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

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

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

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

2.1. The undersigned is not a Prohibited Entity.

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

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

Company

NO SIGNATURE REQUIRED AT THIS TIME

Title

Signature

Date

ATTACHMENT B

Business Associate Agreement

1. Definitions

General definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

- (a) Business Associate. “Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean the Provider, Consultant or entity contracting with the State of South Dakota as set forth more fully in the Agreement this Business Associate Agreement is attached.
- (b) CFR. “CFR” shall mean the Code of Federal Regulations.
- (c) Covered Entity. “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean South Dakota Department of Social Services.
- (d) Designated Record Set. “Designated Record Set” shall have the meaning given to such term in 45 CFR 164.501.
- (e) HIPAA Rules. “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164 (Subparts A, C, D and E). More specifically, the “Privacy Rule” shall mean the regulations codified at 45 CFR Part 160 and Part 164 (Subparts A and E), and the “Security Rule” shall mean the regulations codified at 45 CFR Part 160 and Part 164 (Subparts A and C).
- (f) Protected Health Information. “Protected Health Information” or “PHI” shall mean the term as defined in 45 C.F.R. §160.103, and is limited to the Protected Health Information received from, or received or created on behalf of Covered Entity by Business Associate pursuant to performance of the Services under the Agreement.

2. Obligations and Activities of Business Associate

Business Associate agrees to:

- (a) Not Use or Disclose Protected Health Information other than as permitted or required by the Agreement or as Required by Law;
- (b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic Protected Health Information, to prevent Use or Disclosure of Protected Health Information other than as provided for by the Agreement;
- (c) Report to covered entity any Use or Disclosure of Protected Health Information not provided for by the Agreement of which it becomes aware, including Breaches of Unsecured Protected Health Information as required at 45 CFR 164.410, and any Security Incident of which it becomes aware within five (5) business days of receiving knowledge of such Use, Disclosure, Breach, or Security Incident;
- (d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any Subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;
- (e) Make available Protected Health Information in a designated record set to the covered entity as necessary to satisfy covered entity’s obligations under 45 CFR 164.524. Business associate shall cooperate with covered entity to fulfill all requests by Individuals for access to the Individual’s Protected Health Information that are approved by covered entity. If business associate receives a request from an Individual for access to Protected Health Information, business associate

shall forward such request to covered entity within ten (10) business days. Covered entity shall be solely responsible for determining the scope of Protected Health Information and Designated Record Set with respect to each request by an Individual for access to Protected Health Information;

- (f) Make any amendment(s) to Protected Health Information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526. Within ten (10) business days following any such amendment or other measure, business associate shall provide written notice to covered entity confirming that business associate has made such amendments or other measures and containing any such information as may be necessary for covered entity to provide adequate notice to the Individual in accordance with 45 CFR 164.526. Should business associate receive requests to amend Protected Health Information from an Individual, Business associate shall cooperate with covered entity to fulfill all requests by Individuals for such amendments to the Individual's Protected Health Information that are approved by covered entity. If business associate receives a request from an Individual to amend Protected Health Information, business associate shall forward such request to covered entity within ten (10) business days. Covered entity shall be solely responsible for determining whether to amend any Protected Health Information with respect to each request by an Individual for access to Protected Health Information;
- (g) Maintain and make available the information required to provide an accounting of Disclosures to the covered entities necessary to satisfy covered entity's obligations under 45 CFR 164.528. Business associate shall cooperate with covered entity to fulfill all requests by Individuals for access to an accounting of Disclosures that are approved by covered entity. If business associate receives a request from an Individual for an accounting of Disclosures, business associate shall immediately forward such request to covered entity. Covered entity shall be solely responsible for determining whether to release any account of Disclosures;
- (h) To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and
- (i) Make its internal practices, books, and records available to the covered entity and / or the Secretary of the United States Department of Health and Human Services for purposes of determining compliance with the HIPAA Rules.

3. Permitted Uses and Disclosures by Business Associate

- (a) Except as otherwise limited by this Agreement, Business Associate may make any uses and Disclosures of Protected Health Information necessary to perform its services to Covered Entity and otherwise meet its obligations under this Agreement, if such Use or Disclosure would not violate the Privacy Rule if done by the covered entity. All other Uses or Disclosure by Business Associate not authorized by this Agreement or by specific instruction of Covered Entity are prohibited.
- (b) The business associate is authorized to use Protected Health Information if the business associate de-identifies the information in accordance with 45 CFR 164.514(a)-(c). In order to de-identify any information, Business Associate must remove all information identifying the Individual including, but not limited to, the following: names, geographic subdivisions smaller than a state, all dates related to an Individual, all ages over the age of 89 (except such ages may be aggregated into a single category of age 90 or older), telephone numbers, fax numbers, electronic mail (email) addresses, medical record numbers, account numbers, certificate/ license numbers, vehicle identifiers and serial numbers (including license plate numbers, device identifiers and serial numbers), web universal resource locators (URLs), internet protocol (IP) address number, biometric identifiers (including finger and voice prints), full face photographic images (and any comparable images), any other unique identifying number, and any other characteristic or code.
- (c) Business associate may Use or Disclose Protected Health Information as Required by Law.
- (d) Business associate agrees to make Uses and Disclosures and requests for Protected Health Information consistent with covered entity's Minimum Necessary policies and procedures.
- (e) Business associate may not Use or Disclose Protected Health Information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity except for the specific Uses and Disclosures set forth in (f) and (g).
- (f) Business associate may Disclose Protected Health Information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the Disclosures are Required by Law.
- (g) Business associate may provide Data Aggregation services relating to the Health Care Operations of the covered entity.

4. Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

- (a) Covered entity shall notify business associate of any limitation(s) in the Notice of Privacy Practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate's Use or Disclosure of Protected Health Information.
- (b) Covered entity shall notify business associate of any changes in, or revocation of, the permission by an Individual to Use or Disclose his or her Protected Health Information, to the extent that such changes may affect business associate's Use or Disclosure of Protected Health Information.
- (c) Covered entity shall notify business associate of any restriction on the Use or Disclosure of Protected Health Information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate's Use or Disclosure of Protected Health Information.

5. Term and Termination

- (a) Term. The Term of this Agreement shall be effective as of and shall terminate on the dates set forth in the primary Agreement this Business Associate Agreement is attached to or on the date the primary Agreement terminates, whichever is sooner.
- (b) Termination for Cause. Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement.
- (c) Obligations of Business Associate Upon Termination.
 - 1. Except as provided in paragraph (2) of this section, upon termination of this agreement for any reason, business associate shall return or destroy all Protected Health Information received from, or created or received by business associate on behalf of covered entity. This provision shall apply to Protected Health Information that is in the possession of Subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.
 - 2. If business associate determines that returning or destroying the Protected Health Information is infeasible, business associate shall provide to covered entity, within ten (10) business days, notification of the conditions that make return or destruction infeasible. Upon such determination, business associate shall extend the protections of this agreement to such Protected Health Information and limit further Uses and Disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as business associate maintains such Protected Health Information.
- (d) Survival. The obligations of business associate under this Section shall survive the termination of this Agreement.

6. Miscellaneous

- (a) Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.
- (b) Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.
- (c) Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.
- (d) Conflicts. In the event of a conflict in between the terms of this Business Associate Agreement and the Agreement to which it is attached, the terms of this Business Associate Agreement shall prevail to the extent such an interpretation ensures compliance with the HIPAA Rules.

Attachment C

Bureau of Information and Telecommunications Required State Hosted IT Contract Terms

Pursuant to South Dakota Codified Law § 1-33-44, the Bureau of Information and Telecommunications ("BIT") oversees the acquisition of office systems technology, software, and services; telecommunication equipment, software, and services; and data processing equipment, software, and services for departments, agencies, commissions, institutions, and other units of state government. As part of its duties as the Executive Branch's centralized IT agency, BIT requires the contract terms and conditions of this Attachment 2. For purposes of this Attachment, Optum Government Solutions, Inc. will be referred to as the "Consultant."

It is understood and agreed to by all parties that BIT has reviewed and approved only this Attachment. 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 Attachment as being the then current version of the clauses and if any additional required clauses are needed. Changes to clauses in this Attachment must be approved in writing by all parties before they go into effect and a renewal of this Agreement is possible.

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

Section I. Software Functionality and Replacement

The software licensed by the Consultant to the State under this Agreement provides the following: EZG ECM PRO Web Services (Rate Manager), EASYGroup (APC Pro Payment System), WebStrat (APC Pro Payment System and APC Assistant).

The Consultant agrees that:

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

Section II. Provision of Data

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

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

Section III. Threat Notification

Upon becoming aware of a credible security threat with the Consultant's product(s) and or service(s) being used by the State, the Consultant or any subcontractor supplying product(s) or service(s) to the Consultant 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 Consultant will provide the State with information on the threat. 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 Consultant.

Section IV. Security of Code

Any code written or developed by the Consultant, and Consultant's subcontractors, agents, assigns, or affiliated entities must comply with the security requirements of this Agreement.

Section V. Product Support

The State will install and operate the Consultant's product on the State's computing infrastructure. The State will not be responsible for added support costs if the Consultant determines that the Consultant is unable to meet the support commitment(s) given by the Consultant in this Agreement. Any additional costs for support will be borne by the Consultant.

Section VI. Product Usage

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

Section VII. Security

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

By signing this Agreement, the Consultant warrants that:

- A. All Critical, High, Medium, and Low security issues are resolved. Critical, High, 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 Consultant in performing an investigation to determine the nature of any security issues that are discovered or are reasonably suspected after acceptance. The Consultant will fix or mitigate the risk based on the following schedule: Critical and high risk, within 7 days, medium risk within 14 days, low risk, within 30 days.
 - C. All members of the development team have been successfully trained in secure programming techniques.
 - D. A source code control system will be used that authenticates and logs the team member associated with all changes to the software baseline and all related configuration and build files.
 - E. State access to the source code will be allowed to ensure State security standards, policies, and best practices which can be found at <http://bit.sd.gov/standards/>.
 - F. The Consultant will fully support and maintain the Consultant's application on platforms and code bases (including but not limited to: operating systems, hypervisors, web presentation layers, communication protocols, security products, report writers, and any other technologies on which the application depends) that are still being supported, maintained, and patched by the applicable third parties owning them. The Consultant may not withhold support from the State for this application nor charge the State additional fees as a result of the State moving the Consultant's application to a new release of third-party technology if:
 1. The previous version of the third-party code base or platform is no longer being maintained, patched, and supported; and
 2. The new version to which the State moved the application is actively maintained, patched, and supported.

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

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

Section VIII. License to Perform Security Scanning

Before acceptance by the State, the Consultant will provide the State, at a time and for duration agreeable to both parties, access to the application and underlying hardware referenced in this Agreement for security scanning activities. Any scanning performed by the State will not be considered a violation of any licensure agreements the State has with the Consultant or the Consultant has with a third-party. Scanning by the State or any third-party acting for the State will not be considered reverse engineering. If the State's security scanning efforts discover security issues, the State may collaborate, at the State's discretion, with the Consultant on remediation efforts. These remediation efforts will not be considered a violation of any licensure agreements the State has with the Consultant. The State will not be charged for any costs incurred by the Consultant in these remediation efforts unless agreed to by the State in advance in writing. In the

event of conflicting language this clause supersedes any other language in this or any other agreement made between the State and the Consultant.

Section IX. Security Scanning

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

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

Section X. Malicious Code

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

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

During the life of this Agreement the application and hardware can be denied access to or removed from production at the State's discretion. The reasons for the denial of access or removal of the application or hardware from the production system may include but not be limited to security, functionality, unsupported third-party technologies, or excessive resource consumption.

Denial of access or removal of an application or hardware also may be done if scanning shows that any updating or patching of the software and or hardware produces what the State determines are unacceptable results. The Consultant will be liable for additional work required to rectify issues concerning security, functionality, unsupported third-party technologies, and excessive consumption of resources if it is for reasons of correcting security deficiencies or meeting the functional requirements originally agreed to for the application or hardware. At the discretion of the State, contractual payments may be suspended while the application or hardware is denied access to or removed from production. The reasons can be because of the Consultant's actions or inactions. Access to the production system to perform any remedying of the reasons for denial of access or removal of the software and hardware, and its updating and or patching will be made only with the State's prior approval. It is expected that the Consultant will provide the State with proof of the safety and effectiveness of the remedy, update, or patch proposed before the State provides access to the production system. The State will sign a non-disclosure agreement with the Consultant if revealing the update or patch will put the Consultant's intellectual property at risk. If the remedy, update, or patch the Consultant proposes is unable to present software or hardware that meets the State's requirements, as defined by the State, which may include but is not limited to security, functionality, or unsupported third party technologies, to the State's satisfaction within 30 days of the denial of access to or removal from the production system and the Consultant does not employ the change management process to alter the project schedule or deliverables within the same 30 days then at the State's discretion the Agreement may be terminated.

Section XII. Movement of Product

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

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

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

Section XIV. Load Balancing

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

load balanced so that it can operate on the State's computing environment will be at the Consultant's expense.

Section XV. Backup Copies

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

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

Section XVI. Use of Abstraction Technologies

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

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

Section XVII. License Agreements

The Consultant 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 XVIII. Offshore Services

The Consultant will not provide access to State Data to any entity or person(s) located outside the continental United States that are not named in this Agreement 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.

Attachment D

Security and Vendor Questions

Basic Vendor Information

Vendor Legal Name:

Vendor Address:

Directions

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

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

Vendors: The following questions help the State determine the best way to assess and integrate your product or service technology with the State's technology infrastructure. Your response to the questions allows BIT an opportunity to review the security of your product, and helps BIT make an informed decision and recommendation regarding your technology or service. Some questions may not apply to the technology you use. In such cases, simply mark the question as NA (Not Applicable). The questions are divided into sections to help identify the point of the questions.

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

Use the last column as needed to explain your response. Also note, many questions require you to explain your response. The more detailed the response, the better we can understand your product or service.

Where we feel that a Yes/No/NA response is not appropriate, the cell has been grayed out. **If the vendor answers a question by referencing another document or another part of the RFP response, the vendor must provide the page number and paragraph where the information can be found.**

The "BIT" column corresponds to the division within BIT that will be the primary reviewers. If you have questions about the meaning or intent of a question, we can contact the BIT division on your behalf. DC = Data Center; DEV = Development; TEL = Telecommunications; POC = Point of Contact.

System/Product:			
The following questions are relevant for all vendors or third parties engaged in this hardware, software, application, or service.			
		Response	
#	BIT	Question	Select all that apply
1	DC DEV	Is your proposed solution a cloud-based solution or an on-prem solution?	<input type="checkbox"/> State Hosted On-prem (dedicated VM/infrastructure) <input type="checkbox"/> State Cloud Provider (PaaS Solution) <input type="checkbox"/> Vendor Hosted <input type="checkbox"/> Other: (Please state)
2	DC DEV TEL	What type of access is required by vendor or proposed solution to state hosted or external resources?	<input type="checkbox"/> Not Required <input type="checkbox"/> VPN <input type="checkbox"/> API <input type="checkbox"/> SFTP <input type="checkbox"/> Other: (Please state)

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

Section A. System Security

The following questions are relevant for all vendors or third parties engaged in this hardware, application, or service and pertain to relevant security practices and procedures.

				Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed	
A1	DC x	Does the solution require user authentication, and does that authentication solution support OpenID Connect or OAUTH2 to provide single sign-on? Please explain the authentication protocol(s) available to meet the State's single sign-on requirements and how that is implemented with one or more identity providers.					
A2	DC TEL x	Will the system provide internet security functionality on public portals using encrypted network/secure socket layer connections in line with current recommendations of the Open Web Application Security Project (OWASP)?					
A3	POC	Will the system have role-based access?					
A4	DC TEL	Does the application contain mitigations for risks associated to uncontrolled login attempts (response latency, re-Captcha, lockout, IP filtering, multi-factor authentication)? Which mitigations are in place? What are the optional mitigations?					
A5	DC TEL	Are account credentials hashed and encrypted when stored? If "Yes" please describe the encryption used (e.g. SHA256).					
A6	DC TEL x	<p>The protection of the State's system and data is of utmost importance. Web Application Vulnerability Scans must be done if:</p> <ul style="list-style-type: none"> • An application will be placed on the State's system. • The State's system connects to another system. • The contractor hosts State data. • The contractor has another party host State data the State will want to scan that party. <p><u>The State would want to scan a test system; not a production system and will not do penetration testing.</u> The scanning will be done with industry standard tools. Scanning would also take place annually as well as when there are code changes. Will you allow the State to scan a test system? If no, please explain or provide an alternative option to ensure protection of the State's system and data.</p>					
A7	DC	Will SSL traffic be decrypted and inspected before it is allowed into your system?					
A8	POC x	Will organizations other than the State of South Dakota have access to our data?					
A9	DEV TEL	Do you have developers that possess software security related certifications (e.g., the SANS secure coding certifications)?					

A10	DEV	Are there any additional components or configurations required outside of the base product to meet the State's security needs?				
A11	TEL	What threat assumptions were made, if any, when designing protections for the software and information assets processed?				
A12	TEL	How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used?				
A13	TEL	What security criteria, if any, are considered when selecting third party suppliers?				
A14	TEL	How has the software been measured/assessed for its resistance to publicly known vulnerabilities and/or attack patterns identified in the Common Vulnerabilities & Exposures (CVE®) or Common Weakness Enumerations (CWEs)? How have the findings been mitigated?				
A15	TEL	Has the software been evaluated against the Common Criteria, FIPS 140-3, or other formal evaluation process? If so, please describe what evaluation assurance level (EAL) was achieved, what protection profile the product claims conformance to, and indicate if the security target and evaluation report are available.				
A16	DC TEL	Are static or dynamic software security analysis tools used to identify weaknesses in the software that can lead to exploitable vulnerabilities? If yes, which tools are used? What classes of weaknesses are covered? When in the SDLC are these scans performed? Are SwA experts involved in the analysis of the scan results?				
A17	DC TEL x	Has the product undergone any vulnerability or penetration testing? If yes, how frequently, by whom, and are the test reports available under a nondisclosure agreement? How have the findings been mitigated?				
A18	DC	Does your company have an executive-level officer responsible for the security of your company's software products and/or processes?				
A19	DC	How are software security requirements developed?				
A20	DC	What risk management measures are used during the software's design to mitigate risks posed by use of third-party components?				
A21	DC	What is your background check policy and procedure? Are your background checks fingerprint based? If required, would you be willing to undergo fingerprint-based background checks?				
A22	DEV	Does your company have formally defined security policies associated with clearly defined roles and				

		responsibilities for personnel working within the software development life cycle? Explain.				
A23	TEL	What are the policies and procedures used to protect sensitive information from unauthorized access? How are the policies enforced?				
A24	DC TEL	Do you have an automated Security Information and Event Management system?				
A25	DC TEL	What types of event logs do you keep and how long do you keep them?				
		a. System events				
		b. Application events				
		c. Authentication events				
		d. Physical access to your data center(s)				
		e. Code changes				
		f. Other:				
A26	DC	How are security logs and audit trails protected from tampering or modification? Are log files consolidated to single servers?				
A27	DEV	a. Are security specific regression tests performed during the development process?				
		b. If yes, how frequently are the tests performed?				
A28	TEL	What type of firewalls (or application gateways) do you use? How are they monitored/managed?				
A29	TEL	What type of Intrusion Detection System/Intrusion Protection Systems (IDS/IPS) do you use? How are they monitored/managed?				
A30	DC TEL	What are your procedures for intrusion detection, incident response, and incident investigation and escalation?				
A31	DC TEL	Do you have a BYOD policy that allows your staff to put any sort of sensitive or legally protected State data on their device personal device(s) or other non-company owned system(s)?				
A32	DC TEL	Do you require multifactor authentication be used by employees and subcontractors who have potential access to legally protected State data or administrative control? If yes, please explain your practices on multifactor authentication including the authentication level used as defined in NIST 800-63 in your explanation. If no, do you plan on implementing multifactor authentication? If so, when?				

A33	POC	Will this system provide the capability to track data entry/access by the person, date, and time?				
A34	DC DEV POC TEL	Will the system provide data encryption for sensitive or legally protected information both at rest and transmission? If yes, please provide details.				
A35	DC	a. Do you have a SOC 2 or ISO 27001 audit report?				
		b. Is the audit performed annually?				
		c. When was the last audit performed?				
		d. If it is SOC 2 audit report, does it cover all 5 of the trust principles?				
		e. If it is a SOC 2 audit report, what level is it?				
		f. Does the audit include cloud service providers?				
		g. Has the auditor always been able to attest to an acceptable audit result?				
		h. Will you provide a copy of your latest SOC 2 or ISO 27001 audit report upon request? A redacted version is acceptable.				
A36	DC	Do you or your cloud service provider have any other security certification beside SOC 2 or ISO 27001, for example, FedRAMP or HITRUST?				
A37	DC TEL	Are you providing a device or software that can be defined as being Internet of Thing (IoT)? Examples include IP camera, network printer, or connected medical device. If yes, what is your process for ensuring the software on your IoT devices that are connected to the state's system, either permanently or intermittently, are maintained and/or updated?				
A38	DC	Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all registry settings?				
A39	DC	What are your policies and procedures for hardening servers?				
A40	DC TEL	(Only to be used when medical devices are being acquired.) Please give the history of cybersecurity advisories issued by you for your medical devices. Include the device, date, and the nature of the cybersecurity advisory.				
A41	DC POC	Does any product you propose to use or provide the State include software, hardware, or hardware components manufactured by any company on the federal government's Entity List?				

A42	DC	Describe your process for monitoring the security of your suppliers.				
------------	----	--	--	--	--	--

Section B. Hosting

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

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

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

Response						
#	BIT	Question	YES	NO	NA	Explain answer as needed
B1	POC	Are there expected periods of time where the application will be unavailable for use?				
B2	DC	If you have agents or scripts executing on servers of hosted applications what are the procedures for reviewing the security of these scripts or agents?				
B3	DC	What are the procedures and policies used to control access to your servers? How are audit logs maintained?				
B4	DC DEV POC TEL	Do you have a formal disaster recovery plan? Please explain what actions will be taken to recover from a disaster. Are warm or hot backups available? What are the Recovery Time Objectives and Recovery Point Objectives?				
B5	DC	Explain your tenant architecture and how tenant data is kept separately?				
B6	DC	What are your data backup policies and procedures? How frequently are your backup procedures verified?				
B7	DC DEV TEL	If any cloud services are provided by a third-party, do you have contractual requirements with them dealing with: <ul style="list-style-type: none"> • Security for their I/T systems; • Staff vetting; • Staff security training? 				
		a. If yes, summarize the contractual requirements.				
		b. If yes, how do you evaluate the third-party's adherence to the contractual requirements?				
B8	DC	If your application is hosted by you or a third party, are all costs for your software licenses in addition to third-party software (i.e. MS-SQL, MS Office, and Oracle) included in your cost proposal? If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized?				
B9	DC	a. Do you use a security checklist when standing up any outward facing system?				
		b. Do you test after the system was stood up to make sure everything in the checklist was correctly set?				
B10	DC	How do you secure Internet of Things (IoT) devices on your network?				

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

Section C: Database

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

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

Section D: Contractor Process

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

				Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed	
D1	DC POC	Will the vendor provide assistance with installation?					
D2	DC DEV POC TEL	Does your company have a policy and process for supporting/requiring professional certifications? If so, how do you ensure certifications are valid and up-to date?					
D3	DEV	What types of functional tests are/were performed on the software during its development (e.g., spot checking, component-level testing, and integrated testing)?					
D4	DEV	Are misuse test cases included to exercise potential abuse scenarios of the software?					
D5	TEL	What release criteria does your company have for its products regarding security?					
D6	DEV	What controls are in place to ensure that only the accepted/released software is placed on media for distribution?					
D7	DC DEV	a. Is there a Support Lifecycle Policy within the organization for the software					
		b. Does it outline and establish a consistent and predictable support timeline?					
D8	DC	How are patches, updates, and service packs communicated and distributed to the State?					
D9	DEV	What services does the help desk, support center, or (if applicable) online support system offer when are these services available, and are there any additional costs associated with the options?					
D10	DC	a. Can patches and service packs be uninstalled?					
		b. Are the procedures for uninstalling a patch or service pack automated or manual?					
D11	DC DEV	How are enhancement requests and reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, prioritized, and reported? Is the management and reporting policy available for review?					
D12	DC	What are your policies and practices for reviewing design and architecture security impacts in relation to deploying patches, updates, and service packs?					
D13	DC	Are third-party developers contractually required to follow your configuration management and security policies and how do you assess their compliance?					
D14	DEV	What policies and processes does your company use to verify that your product has its comments sanitized and does not contain undocumented functions, test/debug code, or unintended, “dead,” or malicious code? What tools are used?					
D15	DEV	How is the software provenance verified (e.g., any checksums or signatures)?					

D16	DEV	a. Does the documentation explain how to install, configure, and/or use the software securely?				
		b. Does it identify options that should not normally be used because they create security weaknesses?				
D17	DEV	a. Does your company develop security measurement objectives for all phases of the SDLC?				
		b. Has your company identified specific statistical and/or qualitative analytical techniques for measuring attainment of security measures?				
D18	DC	a. Is testing done after changes are made to servers?				
		b. What are your rollback procedures in the event of problems resulting from installing a patch or service pack?				
D19	DC	What are your procedures and policies for handling and destroying sensitive data on electronic and printed media?				
D20	DC TEL	How is endpoint protection done? For example, is virus prevention used and how are detection, correction, and updates handled?				
D21	DC TEL	Do you perform regular reviews of system and network logs for security issues?				
D22	DC	Do you provide security performance measures to the customer at regular intervals?				
D23	DC POC	What technical, installation, and user documentation do you provide to the State? Is the documentation electronically available and can it be printed?				
D24	DC DEV POC	a. Will the implementation plan include user acceptance testing?				
		b. If yes, what were the test cases?				
		c. Do you do software assurance?				
D25	DC DEV POC TEL	Will the implementation plan include performance testing?				
D26	DEV POC	Will there be documented test cases for future releases including any customizations done for the State of South Dakota?				
D27	DEV POC	If the State of South Dakota will gain ownership of the software, does the proposal include a knowledge transfer plan?				
D28	DEV POC	Has your company ever conducted a project where your product was load tested?				
D29	DC	Please explain the pedigree of the software. Include in your answer who are the people, organization, and processes that created the software.				
D30	DC	Explain the change management procedure used to identify the type and extent of changes allowed in the software throughout its lifecycle. Include information on the oversight controls for the change management procedure.				

D31	DC DEV TEL	Does your company have corporate policies and management controls in place to ensure that only corporate-approved (licensed and vetted) software components are used during the development process? Provide a brief explanation. Will the supplier indemnify the acquirer from these issues in the license agreement? Provide a brief explanation.				
D32	DEV	Summarize the processes (e.g., ISO 9000, CMMi), methods, tools (e.g., IDEs, compilers), techniques, etc. used to produce and transform the software.				
D33	DEV	a. Does the software contain third-party developed components?				
		b. If yes, are those components scanned by a static code analysis tool?				
D34	DC DEV TEL	What security design and security architecture documents are prepared as part of the SDLC process? How are they maintained? Are they available to/for review?				
D35	DEV	Does your organization incorporate security risk management activities as part of your software development methodology? If yes, please provide a copy of this methodology or provide information on how to obtain it from a publicly accessible source.				
D36	DC	Does your company ever perform site inspections/policy compliance audits of its U.S. development facilities? Of its non-U.S. facilities? Of the facilities of its third-party developers? If yes, how often do these inspections/audits occur? Are they periodic or triggered by events (or both)? If triggered by events, provide examples of “trigger” events.				
D37	DC TEL	How are trouble tickets submitted? How are support issues, specifically those that are security-related escalated?				
D38	DC DEV	Please describe the scope and give an overview of the content of the security training you require of your staff, include how often the training is given and to whom. Include training specifically given to your developers on secure development.				
D39	DC TEL x	It is State policy that all Contractor Remote Access to systems for support and maintenance on the State Network will only be allowed through Citrix Netscaler. Would this affect the implementation of the system?				
D40	POC TEL x	Contractors are also expected to reply to follow-up questions in response to the answers they provided to the security questions. At the State’s discretion, a contractor’s answers to the follow-up questions may be required in writing and/or verbally. The answers provided may be used as part of the contractor selection criteria. Is this acceptable?				
D41	DC DEV POC TEL x	(For PHI only) a. Have you done a risk assessment? If yes, will you share it?				

		b. If you have not done a risk assessment, when are you planning on doing one?				
		c. If you have not done a risk assessment, would you be willing to do one for this project?				
D42	DEV POC	Will your website conform to the requirements of Section 508 of the Rehabilitation Act of 1973?				

Section E: Software Development

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

				Response		
#	BIT	Question	YES	NO	NA	Explain answer as needed.
E1	DEV POC x	What are the development technologies used for this system?				If marked yes, indicate version.
		ASP.Net				
		VB.Net				
		C#.Net				
		.NET Framework				
		Java/JSP				
		MS SQL				
		Other				
E2	DC TEL	Is this a browser-based user interface?				
E3	DEV POC	Will the system have any workflow requirements?				
E4	DC	Can the system be implemented via Citrix?				
E5	DC	Will the system print to a Citrix compatible networked printer?				
E6	TEL	If your application does not run under the latest Microsoft operating system, what is your process for updating the application?				
E7	DEV	Identify each of the Data, Business, and Presentation layer technologies your product would use and provide a roadmap outlining how your release or update roadmap aligns with the release or update roadmap for this technology.				
E8	TEL x	Will your system use Adobe Air, Adobe Flash, Adobe ColdFusion, Apache Flex, Microsoft Silverlight, PHP, Perl, Magento, or QuickTime? If yes, explain?				
E9	DEV	To connect to other applications or data, will the State be required to develop custom interfaces?				
E10	DEV	To fulfill the scope of work, will the State be required to develop reports or data extractions from the database? Will you provide any APIs that the State can use?				
E11	DEV POC	Has your company ever integrated this product with an enterprise service bus to exchange data between diverse computing platforms?				
E12	DC	a. If the product is hosted at the State, will there be any third-party application(s) or system(s) installed or embedded to support the product (for example, database software, run libraries)?				
		b. If yes, please list those third-party application(s) or system(s).				
E13	DEV	What coding and/or API standards are used during development of the software?				
E14	DEV	Does the software use closed-source Application Programming Interfaces (APIs) that have undocumented functions?				
E15	DEV	How does the software's exception handling mechanism prevent faults from leaving the				

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

F. Infrastructure

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

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed.
F1	DC	Will the system infrastructure have a special backup requirement?				
F2	DC	Will the system infrastructure have any processes that require scheduling?				
F3	DC	The State expects to be able to move your product without cost for Disaster Recovery purposes and to maintain high availability. Will this be an issue?				
F4	TEL x	Will the network communications meet Institute of Electrical and Electronics Engineers (IEEE) standard TCP/IP (IPv4, IPv6) and use either standard ports or State-defined ports as the State determines?				
F5	DC x	It is State policy that all systems must be compatible with BIT's dynamic IP addressing solution (DHCP). Would this affect the implementation of the system?				
F6	TEL x	It is State policy that all software must be able to use either standard Internet Protocol ports or Ports as defined by the State of South Dakota BIT Network Technologies. Would this affect the implementation of the system? If yes, explain.				
F7	DC	It is State policy that all HTTP/SSL communication must be able to be run behind State of South Dakota content switches and SSL accelerators for load balancing and off-loading of SSL encryption. The State encryption is also PCI compliant. Would this affect the implementation of your system? If yes, explain.				
F8	DC x	The State has a virtualize first policy that requires all new systems to be configured as virtual machines. Would this affect the implementation of the system? If yes, explain.				
F9	TEL x	It is State policy that all access from outside of the State of South Dakota's private network will be limited to set ports as defined by the State and all traffic leaving or entering the State network will be monitored. Would this affect the implementation of the system? If yes, explain.				
F10	TEL	It is State policy that systems must support Network Address Translation (NAT) and Port Address Translation (PAT) running inside the State Network. Would this affect the implementation of the system? If yes, explain.				
F11	TEL x	It is State policy that systems must not use dynamic Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports unless the system is a well-known one that is state firewall supported (FTP, TELNET, HTTP, SSH, etc.). Would this affect the implementation of the system? If yes, explain.				
F12	DC	The State of South Dakota currently schedules routine maintenance from 0400 to 0700 on Tuesday mornings for our non-mainframe environments and once a month from 0500 to 1200 for our mainframe				

		environment. Systems will be offline during this scheduled maintenance time periods. Will this have a detrimental effect to the system?				
F13	POC TEL	Please describe the types and levels of network access your system/application will require. This should include, but not be limited to TCP/UDP ports used, protocols used, source and destination networks, traffic flow directions, who initiates traffic flow, whether connections are encrypted or not, and types of encryption used. The Contractor should specify what access requirements are for user access to the system and what requirements are for any system level processes. The Contractor should describe all requirements in detail and provide full documentation as to the necessity of the requested access.				
F14	POC x	List any hardware or software you propose to use that is not State standard, the standards can be found at: https://bit.sd.gov/bit?id=bit_standards_overview .				
F15	DC	Will your application require a dedicated environment?				
F16	DEV POC	Will the system provide an archival solution? If not, is the State expected to develop a customized archival solution?				
F17	DC TEL	Provide a system diagram to include the components of the system, description of the component, and how the components communicate with each other.				
F18	DC	Can the system be integrated with our enterprise Active Directory to ensure access is controlled?				
F19	TEL x	It is State policy that no equipment can be connected to State Network without direct approval of BIT Network Technologies. Would this affect the implementation of the system?				
F20	DC x	Will the server-based software support:				
		a. Windows server 2016 or higher				
		b. IIS7.5 or higher				
		c. MS SQL Server 2016 standard edition or higher				
		d. Exchange 2016 or higher				
		e. Citrix XenApp 7.15 or higher				
		f. VMWare ESXi 6.5 or higher				
		g. MS Windows Updates				
h. Windows Defender						
F21	TEL x	All network systems must operate within the current configurations of the State of South Dakota's firewalls, switches, IDS/IPS, and desktop security infrastructure. Would this affect the implementation of the system?				
F22	DC	All systems that require an email interface must use SMTP Authentication processes managed by BIT Datacenter. Mail Marshal is the existing product used for SMTP relay. Would this affect the implementation of the system?				
F23	DC TEL	The State implements enterprise-wide anti-virus solutions on all servers and workstations as well as controls the roll outs of any and all Microsoft				

		patches based on level of criticality. Do you have any concerns regarding this process?				
F24	DC TEL	What physical access do you require to work on hardware?				
F25	DC	How many of the vendor's staff and/or subcontractors will need access to the state system, will this be remote access, and what level of access will they require?				

Section G: Business Process

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

				Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed.	
G1	DC	a. If your application is hosted on a dedicated environment within the State’s infrastructure, are all costs for your software licenses in addition to third-party software (i.e. MS-SQL, MS Office, and Oracle) included in your cost proposal?					
		b. If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized?					
G2	POC	Explain the software licensing model.					
G3	DC DEV POC	Is on-site assistance available? If so, what is the charge?					
G4	DEV POC	a. Will you provide customization of the system if required by the State of South Dakota?					
		b. If yes, are there any additional costs for the customization?					
G5	POC	Explain the basis on which pricing could change for the State based on your licensing model.					
G6	POC	Contractually, how many years price lock will you offer the State as part of your response? Also, as part of your response, how many additional years are you offering to limit price increases and by what percent?					
G7	POC	Will the State acquire the data at contract conclusion?					
G8	POC	Will the State’s data be used for any other purposes other than South Dakota’s usage?					
G9	DC	Has your company ever filed for Bankruptcy under U.S. Code Chapter 11? If so, please provide dates for each filing and describe the outcome.					
G10	DC	Has civil legal action ever been filed against your company for delivering or failing to correct defective software? Explain.					
G11	DC	Please summarize your company’s history of ownership, acquisitions, and mergers (both those performed by your company and those to which your company was subjected).					
G12	DC	Will you provide on-site support 24x7 to resolve security incidents? If not, what are your responsibilities in a security incident?					
G13	DEV	What training programs, if any, are available or provided through the supplier for the software? Do you offer certification programs for software integrators? Do you offer training materials, books, computer-based training, online educational forums, or sponsor conferences related to the software?					
G14	DC TEL	Are help desk or support center personnel internal company resources or are these services					

		outsourced to third parties? Where are these resources located?				
G15	DC	Are any of the professional services you plan to provide located outside the United States (e.g., help desk or transcription services)?				
G16	DC	Is the controlling share (51%+) of your company owned by one or more non-U.S. entities?				
G17	DC	What are your customer confidentiality policies? How are they enforced?				
G18	DC POC x	Will this application now or possibly in the future share PHI with other entities on other networks, be sold to another party, or be accessed by anyone outside the US?				
G19	DC	If the product is hosted at the State, will there be a request to include an application to monitor license compliance?				
G20	DC POC	Is telephone assistance available for both installation and use? If yes, are there any additional charges?				
G21	DC TEL	What do you see as the most important security threats your industry faces?				