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

Cyber Security and Privacy Assessment Services

PROPOSALS ARE DUE NO LATER THAN MAY 31st, 2022 5:00PM CDT

RFP 2767 **BUYER**: Department of Social Services, Office of the Secretary, Operations office **POC**: Dawson Lewis Dawson.Lewis@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 South Dakota Department of Social Services (DSS) is required by Federal law to conduct security assessments on our various systems. This includes Automatic Data Processing (ADP) systems, Health Information Exchange (HIX) systems, system Penetration testing, and general IT Risks.

The systems belong to the Division of Economic Assistance (EA), Division of Child Support (DCS), and Division of Medical Services. Additional offices may fall under the scope of these assessments.

The Bureau of Information and Telecommunications (BIT) oversees the electronic infrastructure of State government. As such, they will not take the lead in the assessments. However, they will be a resource for the offeror.

Over the past 15 years we have had multiple contracts to perform these services but now seek to consolidate the work in one contract.

Therefore, we are looking for an offeror or offerors who can work with the DSS and BIT to analyze and test our various systems to make sure that we are in compliance with various Federal regulations

1.2 ISSUING OFFICE AND RFP REFERENCE NUMBER

The Operations Office is the issuing office for this document and all subsequent addenda relating to it, on behalf of the State of South Dakota, DSS. The reference number for the transaction is ***RFP 2767***. Refer to this number on all proposals, correspondence, and documentation relating to the RFP.

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

1.3 LETTER OF INTENT

All interested offerors are requested to submit a non-binding Letter of Intent to respond to this RFP. While preferred, a Letter of Intent is not mandatory to submit a proposal. This can be sent via email with the subject line ***RFP 2767 Letter of Intent*** as the subject line

1.4 SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)

RFP Publication	April 19, 2022
Letter of Intent to Respond Due	May 3, 2022
Deadline for Submission of Written Inquiries	May 3, 2022
Responses to Offeror Questions	May 17, 2022
Request for SFTP folder	May 24, 2022
Proposal Submission	May 31, 2022 5:00pm CDT
Oral Presentations/discussions (if required)	TBD
Anticipated Award Decision/Contract Negotiation	June 30, 2022

1.5 SUBMITTING YOUR PROPOSAL

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

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

Proposals shall be submitted as PDFs via Secured File Transfer Protocol (SFTP). Offerors must request an SFTP folder no later than May 24, 2022, by emailing Dawson Lewis at the email indicated on page one. The subject line should be ***RFP 2767 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.

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

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

1.7 NON-DISCRIMINATION STATEMENT

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

1.8 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.

1.9 MODIFICATION OR WITHDRAWAL OF PROPOSALS

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

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

1.10 OFFEROR INQUIRIES

Offerors may email inquiries concerning this RFP to obtain clarification of requirements. No inquiries will be accepted after May 3, 2022. Email inquiries must be sent to Dawson.Lewis@state.sd.us with the following wording, exactly as written, in the subject line: ***RFP 2767 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 May 17, 2022. 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.

1.11 PROPRIETARY INFORMATION

The proposal of the successful offeror(s) becomes public information.

Proprietary information can be protected under limited circumstances such as client lists and non-public financial statements. Pricing and service elements are not considered proprietary. An entire proposal may not be marked as proprietary. ***Offerors must clearly identify in the Executive Summary and mark in the body of the proposal any specific proprietary information they are requesting to be protected***. The Executive Summary must contain specific justification explaining why the information is to be protected. Proposals may be reviewed and evaluated by any person at the discretion of 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.

1.12 LENGTH OF CONTRACT

The contract will begin approximately July 1, 2022, and continue through May 31, 2025. There can be up to four one-year extensions.

1.13 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.

1.14 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. As part of the negotiation process, the contract terms listed in Attachment A may be altered or deleted.

Attachment B are the clauses from the **Bureau of Information and Telecommunications** (BIT). Because we expect a wide range of proposed solutions, we have included the widest number of possible clauses. As part of the negotiation process, the contract terms listed in both attachments may be altered or deleted.
.

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

The following assessments are needed. Social Services would prefer to work with one offeror to do all assessments. Offerors may provide proposals for all four or just selected ones. However, points will be awarded based on how many assessment types are proposed.

DSS has multiple programs that are overseen by various Federal offices which have their own requirements for testing security. For example, Centers for Medicare & Medicaid Services (CMS) requires that a 3rd party completes the Minimum Acceptable Risk Standards for Exchanges (MARS-E) audit every three years whereas the Office of Child Support Enforcement (OCSE) requires the submittal of an annual Security Agreement. This agreement acknowledges the State Child Support Agency complies with the security requirements identified by OCSE, to protect the sensitive data provided through the Federal Parent Locate Services, and child support information in general.

The following sections describe the expectations for an offeror's response and the work which needs to be conducted. The federal guidelines and standards may not be exhaustive and are subject to change.

3.1 General overview of what is expected in the offeror's response

For each of the four Assessment types listed below the Offeror should

- 3.1.1 Start with a summary overview of your understanding of what needs to be done and your methodology for completing the work.
- 3.1.2 Clearly describe their methodology for testing.
  - 3.1.2.1 This should include methodology for testing electronic systems and physical security.
- 3.1.3 As applicable, explain how their methodology will comply with the federal guidelines and standards found in
  - 3.1.3.1 IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies
  - 3.1.3.2 National Institute of Standards and Technology (NIST) 800-30, Guide for Conducting Risk Assessments
  - 3.1.3.3 NIST SP 800-53, Revision 4, Recommended Security Controls for Federal Information Systems and Organizations (Revision 5 starts in September 2022)
  - 3.1.3.4 The Security Content Automation Protocol (SCAP)
  - 3.1.3.5 Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules
  - 3.1.3.6 Minimum Acceptable Risk Standards for Exchanges (MARS-E)
  - 3.1.3.7 CMS Streamlined Modular Certification for Medicaid Enterprise Systems Certification Guidance, Appendix D "Independent Third-Party Security and Privacy Assessment Guidelines for Medicaid Enterprise Systems", pages 41-52. This is found here: https://www.medicaid.gov/medicaid/data-and-systems/downloads/smc-certification-guidance.pdf
  - 3.1.3.8 Others as applicable

3.2 General IT Risk Assessment

This includes assessment of both physical processes and IT assets

- 3.2.1 Overview
  - 3.2.1.1 The Risk Assessment to include both physical and electronic assets

3.2.1.2 To be done yearly

3.2.1.3 First Assessment report due by September 30, 2022

3.2.1.4 A list of controls and policies reviewed in previous year will be provided to winning bidders.

3.2.2 DSS expects the offeror's response to include

3.2.2.1 Provide a list of what they understand to be the applicable Federal and/or Industry standards. And why they apply.

3.2.2.2 Describe how they will aid DSS in the discovery process to find any systems or assets that may have been missed in the initial list we provide.

3.2.2.3 Describe their methodology for how they would determine the risks/threats for each.

3.2.2.4 What roles they expect DSS and BIT to have in providing information to them.

3.2.2.5 Outline and describe how they would audit/test/review to ensure that we meet those standards.

3.3 Automated Data Processing (ADP) systems assessment

The risk analysis will assist the state by measuring the ADP system's vulnerability to fraud or theft, loss of data, physical destruction, unauthorized access, intrusion and harm to agency activities.

3.3.1 Overview

3.3.1.1 Federal guidelines can be found in

3.3.1.1.1 45 CFR Subtitle A Subchapter A § 95.601 onwards

3.3.1.1.2 45 CFR § 95.621 for specific review standards

3.3.1.1.3 Additional information is identified in program specific information under 45 CFR and 42 U.S.C.

3.3.1.2 To include

3.3.1.2.1 Physical security of ADP resources

3.3.1.2.2 Equipment security to protect equipment from theft and unauthorized use

3.3.1.2.3 Software and data security

3.3.1.2.4 Telecommunications security

3.3.1.2.5 Personnel security

3.3.1.2.6 Contingency plans to meet critical processing needs in the event of short or long-term interruption of service

3.3.1.2.7 Emergency preparedness

3.3.1.2.8 Designation of an Agency ADP Security Manager

3.3.1.3 Audit to be done biennially

3.3.1.4 First Assessment due by September 30, 2022,

3.3.2 DSS expects the offeror response to

3.3.2.1 Outline their understanding of the relevant Federal security standards that apply to ADP systems.

3.3.2.2 Describe how they will aid DSS in the discovery process to find any systems or assets that may have been missed in the initial list we provide.

3.3.2.3 Outline and describe how they would audit/test systems to ensure that we meet those standards. This should include

3.3.2.3.1 Types of systems you expect to audit. Including both physical and electronic

3.3.2.4 Describe their methodology for how they would determine the risks/threats for each.

3.4 Penetration Testing of the Network and of Web Applications

Penetration testing from outside of the State system is required by CMS for Medical Services and the Medicaid system and by the IRS for FTI information under the control of Economic Assistance and Child Support.

3.4.1 Overview

3.4.1.1 Annual Assessment

3.4.1.2 First Assessment due by September 30, 2022,

3.4.1.3 A list of web pages and apps reviewed in previous year will be provided to winning bidders.

3.4.2 DSS expects the offeror response to

3.4.2.1 Specify what Federal and/or Industry standards their testing will be based on.
For example,
- Penetration Testing Execution Standard (PTES), www.pentest-standard.org
- OWASP Top 10, OWASP Top 10:2021

List the standards you feel are applicable

3.4.2.1.1 Break this out between Network and Web applications where applicable

3.4.2.2 Identify the types of general network vulnerabilities they will be testing for and possible tools they will use.

3.4.2.3 Specify what vulnerabilities in Web applications they will be testing for along with possible tools.

3.4.2.4 Provide a detailed description of their methodology in testing.

3.4.2.4.1 Specify if they will use “Black box” and/or “White Box” testing.

3.4.2.5 Discuss how they would work with BIT to ensure that all potential web pages/applications are included. The focus of this should be the methodology of the search process.

3.5 **Minimum Acceptable Risk Standards for Exchanges (MARS-E)**

3.5.1 Overview

3.5.1.1 Provide an independent third-party security and privacy assessment of the State’s Medicaid Eligibility & Enrollment (E&E) System Security Plan (SSP) in accordance with the CMS Framework for Independent Assessment of Security and Privacy Controls guidance in Appendix A

3.5.1.1.1 Audits are normally done every three years, but circumstances will require two audits in a condensed period.

3.5.1.1.2 First audit of Legacy E&E system due by November 30, 2022

3.5.1.1.3 A second audit due by May 31, 2023, as a result of the implementation of a new Modernized E&E system.

3.5.2 DSS expects the offeror response to

3.5.2.1 Outline how the offeror will assist the State in completing the Security and Privacy Assessment Plan (SAP) in accordance with CMS guidance in Appendix B

3.5.2.2 Describe the offeror's approach to conducting an assessment of all applicable controls and completing the Security and Privacy Assessor Workbook (SAW) in Appendix C

3.5.2.2.1 Methodology for identifying system boundary

3.5.2.2.2 Methodology for completion of the actual audit

3.5.2.2.2.1 Expectations include but not limited to security control testing, penetration testing, network and component scanning, configuration assessment, documentation reviews, personnel interviews, and observations.

3.5.2.3 Outline the Offeror's approach to completing the Security Audit Report (SAR) in accordance with CMS guidance in Appendix D

3.6 Management Tools

It is important to DSS that we have a tool or tools to help us manage the process and to generate reports as needed.

Discuss what tools and capabilities you would provide so that we would have the ability to

3.6.1 Edit the list of what should be tested.

3.6.2 Define testing standards to be used.

3.6.3 Edit vulnerability levels assigned to controls and/or applications.

3.6.4 Edit acceptable risk percentage for controls and/or applications.

3.6.5 Offeror should include other features.

3.6.6 DSS may request a demo of these tools. TBD

3.7 **Reporting Tools**

What reporting tools we have to be able to communicate findings to our Federal and IT partners.

3.7.1 Reports should be understandable for both technical and non-technical staff

3.7.2 Include information on the ability for us to customize reports

3.7.3 Include information on what customization services you provide and at what cost

3.7.4 The ability to customize reports by Division to meet requirements of Federal partners. For example, Child Protection may have different reporting needs than Medicaid.

3.7.5 Provide a list and samples of any existing reports you would include with the reporting tool.

3.7.6 DSS may request a demo of these tools. TBD

3.8 **Remediation Recommendations**
If security issues are found, we would expect an offeror to provide recommendations to remediate those issues. This includes providing test results of failed user specific activities to determine level of failure and appropriate outcomes.

3.8.1 Is this a service is offered?

3.8.2 In order to evaluate an offerors' ability to do this please provide examples where this has been done. Obviously, the examples cannot include details that would compromise the security and privacy of a previous client. Therefore, we expect your response to be somewhat vague on details. Something along the line of "we discovered Vulnerability X with their network protocols. We provided suggestions as to how to remediate the issue that would work with their existing technology. We then followed up with their staff and continued testing, working with their staff to ensure that the new technology was properly implemented."

An offeror may share three to five such examples. In addition, they can provide a simple listing such as, "we have worked with 27 entities to provide remediations services on over 600 issues that need remediation."

4.0 PROPOSAL REQUIREMENTS AND COMPANY QUALIFICATIONS

4.1 The offeror is cautioned that it is the offeror's sole responsibility to submit information related to the evaluation categories and that the State of South Dakota is under no obligation to solicit such information if it is not included with the proposal. The offeror's failure to submit such information may cause an adverse impact on the evaluation of the proposal.

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

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

4.4 Provide the following information related to at ***least*** three previous and/or current service/contracts performed by the offeror's organization which are similar to the requirements of this RFP. You may submit as many as 10 organizations as references. Include this information as well for any service/contract that has been terminated, expired or not renewed in the past three years:

4.4.1 Information needed for references.

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

4.4.1.2 Dates of the service/contract; and

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

4.4.1.4 Type of service provided

4.5 The offeror must submit information that demonstrates their availability and familiarity with the locale in which the project (s) are to be implemented. This should include information on remote staff availability. If you do not have experience within South Dakota, please include information on working with similar size organizations and/or organizations in the upper mid-west.

4.6 The offeror must detail examples that document their ability and proven history in handling special project constraints. Specifically, we are looking for examples where your company and provide extraordinary effort to meet a client's requirement. Examples include coming into to take over a project that had failed or a client cutting the budget.

4.7 The offeror must describe their proposed project management techniques in terms of how they will manage their staff and interactions with State staff.

4.8 If an offeror's proposal is not accepted by the State, the proposal will not be reviewed/evaluated. Reasons for not accepting include but not limited to not being received on time; not the correct format; failure to include requested sections.

5.0 PROPOSAL RESPONSE FORMAT

5.1 Only a PDF copy shall be submitted.

5.1.1 As outlined in section 1.5 "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 All proposals must be organized and have a separator page between each the following headings. The separator page should have the heading names on it.

5.2.1 **RFP Form**. The State's Request for Proposal form completed and signed.

5.2.2 **Executive Summary.** The 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.

For each area of work outlined in Sections 3.2 through 3.7

5.2.3.2.1 Have a separator page between each of the sections. This should be a new page separate from the previous section so that it is clearly delineated what the following pages deal with.

5.2.3.2.2 If you choose to not propose for an assessment type, please include a page that states that.

5.2.3.2.3 An executive summary showing your understanding of the work to be done.

5.2.3.2.4 Answers to the SOW items as listed.

5.2.3.2.5 For each Section include the applicable sample reports. You may also include screenshots of the management tool as applicable.

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.

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 Cost proposal.

6.1.5 Proposed project management techniques;

6.1.6 Ability and proven history in handling special project constraints, and

6.1.7 Familiarity with the project locale;

6.1.8 Availability to the project locale;

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

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

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

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

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

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

6.5.3 Only the response of the offeror awarded work becomes public. Responses to work orders for offerors not selected and the evaluation criteria and scoring for all proposals are not public. Offerors may submit a redacted copy with the full proposal as stated in Section 1.11 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 Format

7.1.1 For each required assessment listed in the Scope of Work indicate the cost as a lump sum for each year performed.

For example, the IT Risk Assessment should be done yearly so indicate the costs for each year.

7.1.2 If you have any optional services proposed, please list each as a separate cost item.

7.1.3 If your firm's normal method is to work hourly, then provide an estimate for the number of hours and the rate then calculate the lump sum.

ATTACHMENT A – Sample Contract

The following through page 25 is provided as a sample and may be subject to change. As stated in section 2 please note any clauses that you have objections to or desire to modify.

STATE OF SOUTH DAKOTA
DEPARTMENT OF SOCIAL SERVICES
DIVISION OF ECONOMIC ASSISTANCE

Consultant Contract
For Consultant Services
Between

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

Referred to as Consultant

Referred to as State

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

1. CONSULTANT'S South Dakota Vendor Number is .

2. PERIOD OF PERFORMANCE:
   This Agreement shall be effective as of June 1, 2021 and shall end on May 31, 2022, unless sooner terminated pursuant to the terms hereof.

   Agreement is the result of request for proposal process, RFP #2767

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

      2. Does this Agreement involve Protected Health Information (PHI)? YES ( ) NO (X)
         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 use state equipment, supplies or facilities.

   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.

      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:
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. 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.

10. 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.

11. 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 for cause 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.

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

13. 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.

14. 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.

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

16. IT STANDARDS:
Any software or hardware provided under this Agreement will comply with state standards which can be found at http://bit.sd.gov/standards/.

17. 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.

18. 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.

19. 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.

20. 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.

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

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

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.

B. Business Automobile Liability Insurance:
Consultant shall maintain business automobile liability insurance or an equivalent form with a limit of not less than $500,000 for each accident. Such insurance shall include coverage for owned, hired, and non-owned vehicles.

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

D. Professional Liability Insurance:
Consultant agrees to procure and maintain professional liability insurance with a limit not less than $1,000,000.

(Medical Health Professional shall maintain current general professional liability insurance with a limit of not less than one million dollars for each occurrence and three million dollars in the aggregate. Such insurance shall include South Dakota state employees as additional insureds in the event a claim, lawsuit, or other proceeding is filed against a state employee as a result of the services provided pursuant to this Agreement. If insurance provided by Medical Health

Professional is provided on a claim made basis, then Medical Health Professional shall provide "tail" coverage for a period of five years after the termination of coverage.)

23. 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.

24. 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.

25. 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.

26. 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.

27. 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").

28. 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).

29. 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.

30. THE STATE OF SOUTH DAKOTA TECHNOLOGY OVERSIGHT
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. BIT requires the contract provisions which are attached to this Agreement as Attachment B and incorporated into this Agreement by reference. It is understood and agreed to by all parties that BIT, as the State's technology governing organization, has reviewed only Attachment B of this agreement. Before renewal of this Agreement BIT must review and approve Attachment B as still being current. BIT's evaluation of Attachment B will be based on changes in the IT security or regulatory requirements. Changes to Attachment B must be approved in writing by all parties before they go into effect and a renewal of this Agreement is possible. The most current version of the State's Information Technology Security Policy will also be provided to the Consultant with the understanding that the Consultant will adhere to the most current State IT security policies.

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

Consultant Signature	Date
Consultant Printed Name	
State - DSS Division Director	Date
State - DSS Chief Financial Officer Jason Simmons	Date
State – DSS Cabinet Secretary Laurie R. Gill	Date
State – BIT Commissioner Jeffrey Clines	Date

State Agency Coding:

CFDA #				
Company				
Account				
Center Req				
Center User				
Dollar Total				

DSS Program Contact Person _____
Phone _____

DSS Fiscal Contact Person Contract Accountant
Phone 605 773-3586

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

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

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

ATTACHMENT B - Bureau of Information and Telecommunications (BIT) Contract clauses.

BIT is charged by the state with making sure that all technology used is compatible with State Standards. Also, that the data of our citizens is safeguarded. Because we do not know what methods an offeror will use to access data we have included the widest possible number of clauses.

Depending on your proposed solution certain of these clauses may not be needed and will be removed from the final contract.

1. CONSULTANT ELECTION NOT TO RENEW CONTRACT OR TO INCREASE FEES
The Consultant is obligated to give the State one hundred and eighty (180) days written notice in the event the Consultant intends not to renew the contract or intends to raise any fees or costs associated with the Consultant's products or services in a subsequent contract unless such fees or costs have previously been negotiated and included in this contract.

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

3. SECURING OF DATA
All facilities used to store, and process State's data will employ industry best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the Consultant's own data of a similar type, and in no event less than commercially reasonable in view of the type and nature of the data involved. Without limiting the foregoing, the Consultant warrants that all State's data will be encrypted in transmission (including via web interface) and storage at no less than AES256 level encryption with SHA256 or SHA2 hashing,

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

5. IMPORT AND EXPORT OF DATA
The State shall have the ability to import or export data piecemeal or in entirety at its discretion without interference from the Consultant. This includes the ability for the State to import or export data to/from other Consultants.

6. PASSWORD PROTECTION
The website(s) and or service(s) that will be hosted by the Consultant for the State will be password protected. If the Consultant provides the user with a preset or default password that password cannot include any Personally Identifiable Information, data protected under the Family Educational Rights and Privacy Act, Protected Health Information, Federal Tax Information or any information defined under state statute as Confidential Information or fragment thereof.

7. MOVEMENT OF PROTECTED STATE DATA
Any State data that is protected by Federal or State statute or requirements or by industry standards must be kept secure. When protected State data is moved to any of the Consultant's production or non-production systems, security must be maintained. The Consultant will ensure that that data will at least have the same level of security as it had on the State's environment. The State's security policies can be found in the Information Technology Security Policies (ITSP).

8. MULTIFACTOR AUTHENTICATION FOR HOSTED SYSTEMS
If the Consultant is hosting on their system or performing Software as a Service where there is the potential for the Consultant and/or the Consultant's subcontractor to see protected State data, then Multifactor Authentication (MFA) must be used to before this data can be accessed. The Consultant's MFA, at a minimum must adhere to the requirements of *Level 3 Authentication Assurance for MFA* as defined in NIST 800-63.

9. 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 (2) 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 one or more aspects of a system that is holding State data, or a product provided by the Consultant.

10. SECURITY INCIDENT NOTIFICATION

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

A. The Consultant shall notify the State Contact within twelve (12) hours of the Consultant becoming aware that a Security Incident has occurred.

   If notification of a Security Incident to the State Contact is delayed because it may impede a criminal investigation or jeopardize homeland or federal security, notification must be given to the State within twelve (12) hours after law-enforcement provides permission for the release of information on the Security Incident.

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

C. At the State's discretion within 48 hours the consultant must provide to the State all data available including: (i) Name of and contact information for the Consultant's Point of Contact for the Security Incident: (ii) date and time of the Security Incident; (iii) date and time the Security Incident was discovered: (iv) description of the Security Incident including the data involved, being as specific as possible; (v) the potential number of records, and if unknown the range of records; (vi) address where the Security Incident occurred: and, (vii) the nature of the technologies involved. Notifications must be sent electronically and encrypted via NIST or other applicable federally approved encryption techniques. If there are none use AES256 encryption. Consultant shall use the term "data incident report" in the subject line of the email. If not all of the information is available for the notification within the specified time period Consultant shall provide the State with all of the available information along with the reason for the incomplete information. A delay in excess of twelve (12) hours is acceptable only if it is necessitated by other legal requirements.

D. If the information from the Breach of System Security includes State of South Dakota residents whose personal or protected information was, or is reasonably believed to have been, acquired by an unauthorized person consultant must notify the resident(s) in accordance with South Dakota Codified Law (SDCL) Chapter 22-40. Requirements of this chapter include that if there are two-hundred and fifty (250) or more residents' records involved the State of South Dakota Attorney General (ATG) must be notified. Both notifications must be within sixty (60) days of the discovery of the breach. The Consultant shall also notify, without unreasonable delay, all consumer reporting

agencies, as defined under 15 U.S.C. § 1681a in effect as of January 1, 2018, and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notice. The Consultant is not required to make a disclosure under this section if, following an appropriate investigation and notice to the ATG, the Consultant reasonably determines that the breach will not likely result in harm to the affected person. The Consultant shall document the determination under this section in writing and maintain the documentation for not less than three (3) years. These statements of requirements from SDCL 22-40 are neither comprehensive nor all inclusive, and consultant shall comply with all applicable provisions of that chapter.

The requirements of section D do not replace the requirements of sections A, B and C but are in addition to them.

11. HANDLING OF SECURITY INCIDENT

For Security Incidents of protected non-health information under the Consultant's control and at the State's discretion the Consultant will preserve all evidence regarding a security incident including but not limited to communications, documents, and logs. The Consultant will also:

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

If, at the State's discretion the Security Incident was due to the actions or inactions of the Consultant and at the Consultant's expense the Consultant will use a credit monitoring service, call center, forensics company, advisors, or public relations firm whose services are acceptable to the State. At the State's discretion the Consultant shall offer two years of credit monitoring to each person whose data was compromised. The State will set the scope of any investigation. The State can require a risk assessment for which the Consultant, the State will mandate the methodology and the scope. At the State's discretion a risk assessment may be performed by a third party at the Consultant's expense.

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

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

12. SECURITY INCIDENTS REGARDING PROTECTED HEALTH INFORMATION

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

Notwithstanding any other provision of this Agreement and in addition to any other remedies available to the State under law or equity, in the event the investigation or review determines that the consultant is responsible for the Security Incident, and where the State incurs any costs in the investigation, review or remediation of the Security Incident, the Consultant shall reimburse the State in full for all such costs. Costs include, but are not limited to, providing notification to regulatory

agencies or other entities as required by law or contract. In the event the investigation or review determines that the consultant is responsible for the Security Incident, the Consultant shall also pay any and all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident, and all costs associated with the remediation of the Consultant's services and/or product(s).

13. SECURITY ACKNOWLEDGEMENT FORM

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

14. BACKGROUND CHECKS

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

15. SECURITY

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

By signing this agreement, the Consultant warrants that:

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

B. Assistance will be provided to the State by the Consultant in performing an investigation to determine the nature of any security issues that are discovered or are reasonably suspected after acceptance. The Consultant will fix or mitigate the risk based on the following schedule: Critical and high risk, within 7 days, medium risk within 14 days, low risk, within 30 days.
C. State technology standards, policies, and best practices will be followed. State technology standards can be found at http://bit.sd.gov/standards/.

16. 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 the written permission of the State. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States.

17. CONSULTANT TRAINING REQUIREMENTS

The Consultant, Consultant's employee(s), and Consultant's Subcontractors, Agents, Assigns, Affiliated Entities and their employee(s), must successfully complete, at the time of hire and annually thereafter, a cyber-security training program. The training must include but is not limited to: i) Legal requirements for handling data, ii) Media sanitation, iii) Strong password protection, iv) Social engineering, or the psychological manipulation of persons into performing actions that are inconsistent with security practices or that cause the divulging of confidential information, and v) Security incident response, and vi) Protected Health Information.

18. BANNED HARDWARE

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

19. REMOTE ACCESS

The Consultant shall prohibit its employees, agents, affiliates and subcontractors from accessing State data remotely except as necessary to provide the services under this Agreement and consistent with all contractual and statutory requirements. The accounts used for remote access cannot be shared accounts and must include multifactor authentication.

APPENDIX A - Framework for the Independent Assessment of Security and Privacy Controls

This document outlines how assessments should be conducted. It can be downloaded as Appendix A

APPENDIX B – CMS Security and Privacy Assessment Plan (SAP) template

As part of this contract a vendor will work with DSS to complete a Security and Privacy Assessment Plan (SAP) plan before the assessment work will begin. The template is presented to help offerors plan their workflow. The full template can be downloaded as Appendix B

APPENDIX C – Security and Privacy Assessor Workbook (SAW)

This is a multi-tab Excel worksheet to be filled out as part of the assessment. The template is presented to help offerors plan their workflow. The full template can be downloaded as Appendix C.

APPENDIX D - Administering Entity Security and Privacy Assessment Report (SAR)

Template for how to report back findings. It can be downloaded as Appendix D

ATTACHMENT C BIT – Security and Contractor Questions

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

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

Contractors: The following questions help the state determine the best way to assess and integrate your product or service technology with the state's technology infrastructure. Some questions may not apply to the technology you use. In such cases, simply mark the question as NA (Not Applicable). You will see that these questions are divided into sections to help identify the point of the questions.
Use the last column as needed to explain your answers. Also note that many questions require you to explain your response. The more detailed the response, the better we can understand your product or service.

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

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

Offerors can request a Word Version by contacting Dawson Lewis at Dawson.Lewis@state.sd.us

Section A: System Security

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

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
A1	DC	If there is a website that is used by State employees or the public as part of the Offeror 's solution the website must use SAML or OAUTH2 to provide single-sign-on.				
A2	DC TEL x	Will the system provide Internet security functionality on public portals using encrypted network/secure socket layer connections in line with current recommendations of the Open Web Application Security Project (OWASP)?				
A3	POC	Will the system have role-based access?				

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

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
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 140-2, or other formal evaluation process? If so, please describe what evaluation assurance level (EAL) was achieved, what protection profile the product claims conformance to, and indicate if the security target and evaluation report are available.				
A16	DC TEL	Are static or dynamic software security analysis tools used to identify weaknesses in the software that can lead to exploitable vulnerabilities? If yes, which tools are used? What classes of weaknesses are covered? When in the SDLC are these scans performed? Are SwA experts involved in the analysis of the scan results?				
A17	DC TEL x	Has the product undergone any vulnerability and/or penetration testing? If yes, how frequency, by whom, and are the test reports available under a nondisclosure agreement? How have the findings been mitigated?				
A18	DC	Does your company have an executive-level officer responsible for the security of your company's software products and/or processes?				
A19	DC	How are software security requirements developed?				
A20	DC	What risk management measures are used during the software's design to mitigate risks posed by use of third-party components?				
A21	DC	What is your background check policy and procedure?				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
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/escalation?				
A31	DC TEL	Do you have a BYOD policy that allows your staff to put any sort of sensitive or legally protected State data on their device personal device(s) or other non-company owned system(s)?				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
A32	DC TEL	Do you require multifactor authentication be used by employees and subcontractors who have potential access to legally protected State data or administrative control? If yes, please explain your practices on multifactor authentication including the authentication level used as defined in NIST 800-63 in your explanation. If no, do you plan on implementing multifactor authentication? If so, when?				
A33	POC	Will this system provide the capability to track data entry/access by the person, date and time?				
A34	DC DEV POC TEL	Will the system provide data encryption for sensitive or legally protected information both at rest and transmission? If yes, please provide details.				
A35	DC	a. Do you have a SOC 2 or ISO 27001 audit report?				
		b. Is the audit done annually?				
		c. If it is SOC 2 audit report, does it cover all 5 of the trust principles?				
		d. If it is a SOC 2 audit report, what level is it?				
		e. Does the audit include cloud service providers?				
		f. Has the auditor always been able to attest to an acceptable audit result?				
		g. Will you provide a copy of your latest SOC 2 or ISO 27001 audit report upon request, a redacted version is acceptable?				
A36		Do you or your cloud service provider have any other security certification beside SOC 2 or ISO 27001, for example, FedRAMP or ITTRUST?				
A37	DC TEL	Are you providing a device or software that can be defined as being Internet of Thing (IoT)? Examples include IP camera, network printer, or connected medical device. If yes, what is your process for ensuring the software on your IoT devices that are connected to the state's system, either permanently or intermittently, are maintained and/or updated?				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
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 US Commerce Department's Entity List?				
A42	DC	Describe your process for monitoring the security of your suppliers.				

Section B: Hosting

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

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
B1	POC	Typically, the State of South Dakota prefers to host all systems. In if the State decides that it would be preferable for the vendor to host the system, is this an option?				
B2	POC	Are there expected periods of time where the application will be unavailable for use?				
B3	DC	If you have agents or scripts executing on servers of hosted applications what are the procedures for reviewing the security of these scripts or agents?				
B4	DC	What are the procedures and policies used to control access to your servers? How are audit logs maintained?				
B5	DC DEV POC TEL	Do you have a formal disaster recovery plan? Please explain what actions will be taken to recover from a disaster. Are warm or hot backups available? What are the Recovery Time Objectives and Recovery Point Objectives?				
B6	DC	Explain your tenant architecture and how tenant data is kept separately?				
B7	DC	What are your data backup policies and procedures? How frequently are your backup procedures verified?				
B8	DC DEV TEL	If any cloud services are provided by a third-party, do you have contractual requirements with them dealing with: · Security for their I/T systems; · Staff vetting; · Staff security training?				
		a. If yes, summarize the contractual requirements.				
		b. If yes, how do you evaluate the third-party's adherence to the contractual requirements?				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
B9	DC	If your application is hosted by you or a third party, are all costs for your software licenses in addition to third-party software (i.e. MS-SQL, MS Office, and Oracle) included in your cost proposal? If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized?				
B10	DC	a. Do you use a security checklist when standing up any outward facing system?				
		b. Do you test after the system was stood up to make sure everything in the checklist was correctly set?				
B11	DC	How do you secure Internet of Things (IoT) devices on your network?				
B12	DC TEL	Do you use Content Threat Removal to extract and transform data?				
B13	DC TEL	Does your company have an endpoint detection and response policy?				
B14	DC TEL	Does your company have any real-time security auditing processes?				
B15	TELE	How do you perform analysis against the network traffic being transmitted or received by your application, systems and/or data center? What benchmarks do you maintain and monitor your systems against for network usage and performance? What process(es) and/or product(s) do you use to complete this analysis, and what results or process(es) can you share?				
B16	TELE	How do you monitor your application, systems and/or data center for security events, incidents or information? What process(es) and/or product(s) do you use to complete this analysis, and what results or process(es) can you share?				
B17	DC TELE	What anti-malware product(s) do you use?				
B18	DC TELE	What is your process to implement new vendor patches as they are released and what is the average time it takes to deploy a patch?				
B19	DC TELE	Have you ever had a data breach? If so, provide information on the breach.				

			Response			
#	BIT	Question	YES	NO	NA	Explanation
B20	POC	Is there a strategy for mitigating unplanned disruptions and what is it?				
B21	DC TEL	What is your process for ensuring the software on your IoT devices that are connected to your system, either permanently or intermittently, is maintained and updated?				
B22	POC	Will the State of South Dakota own the data created in your hosting environment?				
B23	DEV	What are your record destruction scheduling capabilities?				

Section C: Database

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

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

Section D: Contractor Process

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

D1	DC POC	Will the contractor provide assistance with installation?				
D2	DC DEV POC TEL	Does your company have a policy and process for supporting/requiring professional certifications? If so, how do you ensure certifications are valid and up-to date?				
D3	DEV	What types of functional tests are/were performed on the software during its development (e.g., spot checking, component-level testing and integrated testing)?				
D4	DEV	Are misuse test cases included to exercise potential abuse scenarios of the software?				
D5	TEL	What release criteria does your company have for its products regarding security?				
D6	DEV	What controls are in place to ensure that only the accepted/released software is placed on media for distribution?				

			Response			
#	BIT	Question	YES	NO	NA	Explanation
D7	DC DEV	a. Is there a Support Lifecycle Policy within the organization for the software in question?				
		b. Does it outline and establish a consistent and predictable support timeline?				
D8	DC	How are patches, updates and service packs communicated and distributed to the State?				
D9	DEV	What services does the help desk, support center, or (if applicable) online support system offer when are these services available, and are there any additional costs associated with the options?				
D10	DC	a. Can patches and Service Packs be uninstalled?				
		b. Are the procedures for uninstalling a patch or Service Pack automated or manual?				
D11	DC DEV	How are enhancement requests and reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, prioritized and reported? Is the management and reporting policy available for review?				
D12	DC	What are your policies and practices for reviewing design and architecture security impacts in relation to deploying patches, updates and service packs?				
D13	DC	Are third-party developers contractually required to follow your configuration management and security policies and how do you assess their compliance?				
D14	DEV	What policies and processes does your company use to verify that your product has its comments sanitized and does not contain undocumented functions, test/debug code or unintended, “dead,” or malicious code? What tools are used?				
D15	DEV	How is the software provenance verified (e.g. any checksums or signatures)?				

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

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
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	TEL DC DEV	Does your company have corporate policies and management controls in place to ensure that only corporate-approved (licensed and vetted) software components are used during the development process? Provide a brief explanation. Will the supplier indemnify the Acquirer from these issues in the license agreement? Provide a brief explanation.				
D32	DEV	Summarize the processes (e.g., ISO 9000, CMMi), methods, tools (e.g., IDEs, compilers) techniques, etc. used to produce and transform the software.				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
D33	DC DEV	a. Does the software contain third-party developed components?				
		b. If yes, are those components scanned by a static code analysis tool?				
D34	DC DEV TEL	What security design and security architecture documents are prepared as part of the SDLC process? How are they maintained? Are they available to/for review?				
D35	DEV	Does your organization incorporate security risk management activities as part of your software development methodology? If yes, please provide a copy of this methodology or provide information on how to obtain it from a publicly accessible source.				
D36	DC	Does your company ever perform site inspections/policy compliance audits of its U.S. development facilities? Of its non-U.S. facilities? Of the facilities of its third-party developers? If yes, how often do these inspections/audits occur? Are they periodic or triggered by events (or both)? If triggered by events, provide examples of "trigger" events.				
D37	DC TEL	How are trouble tickets submitted? How are support issues, specifically those that are security-related escalated?				
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?				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
D40	POC TEL x	Contractors are also expected to reply to follow-up questions in response to the answers they provided to the security questions. At the State's discretion, a contractor's answers to the follow-up questions may be required in writing and/or verbally. The answers provided may be used as part of the contractor selection criteria. Is this acceptable?				
D41	DC DEV POC TEL x	(For PHI only) a. Have you done a risk assessment? If yes, will you share it?				
		b. If you have not done a risk assessment, when are you planning on doing one?				
		c. If you have not done a risk assessment, would you be willing to do one for this project?				
D42	DEV POC	Will your website conform to the requirements of Section 508 of the Rehabilitation Act of 1973?				

Section E: Software Development

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

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
E1	DEV POC x	What are the development technologies used for this system? Please indicate version as appropriate				
		ASP.Net				
		VB.Net				
		C#.Net				
		.NET Framework				
		Java/JSP				
		MS SQL				
		Other				
E2	DC TEL	Is this a browser-based User Interface?				
E3	DEV POC	Will the system have any workflow requirements?				
E4	DC	Can the system be implemented via Citrix?				
E5	DC	Will the system print to a Citrix compatible networked printer?				
E6	TEL	If your application does not run under the latest Microsoft operating system, what is your process for updating the application?				
E7	DEV	Identify each of the Data, Business and Presentation layer technologies your product would use and provide a roadmap outlining how your release and or update roadmap aligns with the release and or update roadmap for this technology.				
E8	TEL x	Will your system use Adobe Air, Adobe Flash, Adobe ColdFusion, Apache Flex, Microsoft Silverlight, PHP, Perl, Magento, or QuickTime? If yes, explain?				
E9	DEV	To connect to other applications or data, will the State be required to develop custom interfaces?				
E10	DEV	To fulfill the scope of work, will the State be required to develop reports or data extractions from the database? Will you provide any APIs that the State can use?				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
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 so, please list those third-party application(s) or system(s).				
E13	DEV	What coding and/or API standards are used during development of the software?				
E14	DEV	Does the software use closed-source Application Programming Interfaces (APIs) that have undocumented functions?				
E15	DEV	How does the software's exception handling mechanism prevent faults from leaving the software, its resources, and its data (in memory and on disk) in a vulnerable state?				
E16	DEV	Does the exception handling mechanism provide more than one option for responding to a fault? If so, can the exception handling options be configured by the administrator or overridden?				
E17	DEV	What percentage of code coverage does your testing provide?				
E18	DC	a. Will the system infrastructure involve the use of email?				
		b. Will the system infrastructure require an interface into the State's email infrastructure?				
		c. Will the system involve the use of bulk email distribution to State users? Client users? In what quantity will emails be sent, and how frequently?				
E19	TEL x	a. Does your application use any Oracle products?				
		b. If yes, what product(s) and version(s)?				
		c. Do you have support agreements for these applications?				
E20	DC	Explain how and where the software validates (e.g., filter with white listing) inputs from untrusted sources before being used.				

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
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-Source Vulnerability Database (OSVDB)?				
		c. Open Web Application Security Project (OWASP) Top Ten?				
Section F: Infrastructure						
This pertains to how your system interacts with the State's technology infrastructure. If the proposed technology does not interact with the State's system, the questions can be marked as "NA".						
F1	TEL	Is there a workstation install requirement?				
F2	DC	Will the system infrastructure have a special backup requirement?				
F3	DC	Will the system infrastructure have any processes that require scheduling?				
F4	DC	The State expects to be able to move your product without cost for Disaster Recovery purposes and to maintain high availability. Will this be an issue?				
F5	TEL x	Will the network communications meet Institute of Electrical and Electronics Engineers (IEEE) standard TCP/IP (IPv4, IPv6) and use either standard ports or State-defined ports as the State determines?				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
F6	DC x	It is State policy that all systems must be compatible with BIT's dynamic IP addressing solution (DHCP). Would this affect the implementation of the system?				
F7	TEL x	It is State policy that all software must be able to use either standard Internet Protocol ports or Ports as defined by the State of South Dakota BIT Network Technologies. Would this affect the implementation of the system? If yes, explain.				
F8	DC	It is State policy that all HTTP/SSL communication must be able to be run behind State of South Dakota content switches and SSL accelerators for load balancing and off-loading of SSL encryption. The State encryption is also PCI compliant. Would this affect the implementation of your system? If yes, explain.				
F9	DC x	The State has a virtualize first policy that requires all new systems to be configured as virtual machines. Would this affect the implementation of the system? If yes, explain.				
F10	TEL x	It is State policy that all access from outside of the State of South Dakota's private network will be limited to set ports as defined by the State and all traffic leaving or entering the State network will be monitored. Would this affect the implementation of the system? If yes, explain.				
F11	TEL	It is State policy that systems must support Network Address Translation (NAT) and Port Address Translation (PAT) running inside the State Network. Would this affect the implementation of the system? If yes, explain.				
F12	TEL x	It is State policy that systems must not use dynamic Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports unless the system is a well-known one that is state firewall supported (FTP, TELNET, HTTP, SSH, etc.). Would this affect the implementation of the system? If yes, explain.				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
F13	DC	The State of South Dakota currently schedules routine maintenance from 0400 to 0700 on Tuesday mornings for our non-mainframe environments and once a month from 0500 to 1200 for our mainframe environment. Systems will be offline during this scheduled maintenance time periods. Will this have a detrimental effect to the system?				
F14	POC TEL	Please describe the types and levels of network access your system/application will require. This should include, but not be limited to TCP/UDP ports used, protocols used, source and destination networks, traffic flow directions, who initiates traffic flow, whether connections are encrypted or not, and types of encryption used. The Contractor should specify what access requirements are for user access to the system and what requirements are for any system level processes. The Contractor should describe all requirements in detail and provide full documentation as to the necessity of the requested access.				
F15	POC x	List any hardware or software you propose to use that is not State standard, the standards can be found at http://bit.sd.gov/standards/.				
F16	DC	Will your application require a dedicated environment?				
F17	DEV POC	Will the system provide an archival solution? If not, is the State expected to develop a customized archival solution?				
F18	DC TEL	Provide a system diagram to include the components of the system, description of the component and how the components communicate with each other.				
F19	DC	Can the system be integrated with our enterprise Active Directory to ensure access is controlled?				
F20	TEL x	It is State policy that no equipment can be connected to State Network without direct approval of BIT Network Technologies. Would this affect the implementation of the system?				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
F21	DC x	Will the server-based software support: a. Windows server 2016 or higher				
		b. IIS7.5 or higher				
		c. MS SQL Server 2016 standard Edition or higher				
		d. Exchange 2016 or higher				
		e. Citrix XenApp 7.15 or higher				
		f. VMWare ESXi 6.5 or higher				
		g. MS Windows Updates				
		h. Symantec End Point Protection				
F22	TEL x	All network systems must operate within the current configurations of the State of South Dakota's firewalls, switches, IDS/IPS and desktop security infrastructure. Would this affect the implementation of the system?				
F23	DC	All systems that require an email interface must use SMTP Authentication processes managed by BIT Datacenter. Mail Marshal is the existing product used for SMTP relay. Would this affect the implementation of the system?				
F24	DC TEL	The State implements enterprise-wide anti-virus solutions on all servers and workstations as well as controls the roll outs of any and all Microsoft patches based on level of criticality. Do you have any concerns regarding this process?				
F25	DC TEL	What physical access do you require to work on hardware?				
F26	DC	How many of the Vendor's staff and/or subcontractors will need access to the state system, will this be remote access, and what level of access will they require?				

Section G: Business Process

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

			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.				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
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 services you plan to use located offshore (examples include data hosting, data processing, help desk and transcription services)?				
G16	DC	Is the controlling share (51%+) of your company owned by one or more non-U.S. entities?				
G17	DC	What are your customer confidentiality policies? How are they enforced?				
G18	DC POC x	Will this application now or possibly in the future share PHI with other entities on other networks, be sold to another party or be accessed by anyone outside the US?				
G19	DC	If the product is hosted at the State, will there be a request to include an application to monitor license compliance?				
G20	DC POC	Is telephone assistance available for both installation and use? If yes, are there any additional charges?				
G21	DC TEL	What do you see as the most important security threats your industry faces?				

ATTACHMENT D – BIT Security Acknowledgement Form

Security Acknowledgement

Please return agreement to your BIT Manager or Designated BIT Contact

All BIT employees and State contractors must sign; **Agreement to Comply with BIT Information Technology Security Policy (the "Policy").** Users are responsible for compliance to all information security policies and procedures. *By signature below, the employee or contractor hereby acknowledges and agrees to the following:*

1. **Employee is a State of South Dakota employee or contractor that uses non-public State of South Dakota technology infrastructure or information;**
2. **Employee or contractor will protect technology assets of the State from unauthorized activities including disclosure, modification, deletion, and usage;**
3. **Employee or contractor agrees to follow state and federal regulations in regards to confidentiality and handling of data;**
4. **Employee or contractor has read and agrees to abide by the Policy;**
5. **Employee or contractor consents to discuss with a supervisor / State contact regarding Policy violations;**
6. **Employee or contractor shall abide by the policies described as a condition of continued employment / service;**
7. **Employee or contractor understands that any individual found to violate the Policy is subject to disciplinary action, including but not limited to, privilege revocation, employment termination or financial reimbursement to the State;**
8. **Access to the technology infrastructure of the State is a privilege which may be changed or revoked at the discretion of BIT management;**
9. **Access to the technology infrastructure of the State automatically terminates upon departure from the State of South Dakota employment or contract termination;**
10. **Employee or contractor shall promptly report violations of security policies to a BIT manager or State Contact and BIT Help Desk (605.773.4357);**
11. **The Policy may be amended from time to time. The State of South Dakota recommends employees and contractors for the State to regularly review the appropriate Policy and annual amendments.**

Information Technology Security Policy – BIT: http://intranet.bit.sd.gov/policies/
Information Technology Security Policy – CLIENT: http://intranet.bit.sd.gov/policies/
Information Technology Security Policy – CONTRACTOR: http://bit.sd.gov/vendor/default.aspx

Acknowledgement: State of South Dakota Information Technology Security Policy

Contractor: If the individual is signing for their entire company by signing this form the individual affirms that they have the authority to commit their entire organization and all its employees to follow the terms of this agreement.

Employee or Contractor signature Date BIT Manager or Contact Date

Employee or Contractor name and Company name in block capital letters

ATTACHMENT E - BIT Information Technology Security Policy (ITSP)

This is the document referred to in the Security Acknowledgement Form in Attachment D.

It can be downloaded for your review as Attachment E. Please **do not** include this with your response.