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

REQUEST FOR PROPOSALS # 1274

Revenue Website Redevelopment and Maintenance

PROPOSALS ARE DUE NO LATER THAN 5 P.M. CST, FEBRUARY 28, 2018

Contact at the South Dakota Department of Revenue

BUYER: Bobi Adams

EMAIL: Roberta.adams@state.sd.us

Company Information

FIRM NAME: _____ AUTHORIZED SIGNATURE: _____

ADDRESS: _____ TYPE OR PRINT NAME: _____

CITY/STATE: _____ TELEPHONE NO: _____

ZIP (9 DIGIT):_____ FAX NO: _____

FEDERAL TAX ID#:_____ E-MAIL: _____

Company Contact information

Contact name_____ Phone _____

Fax #_____ Email _____

1.0 GENERAL INFORMATION

1.1 PURPOSE OF REQUEST FOR PROPOSAL (RFP)

The purpose of this Request for Proposal ("RFP") is to solicit responders interested in and the costs for coding, programming, designing, launching, and maintaining two new Department of Revenue websites – one Internet and one Intranet. The bid will also include an optional Content Management System (CMS) and associated costs and maintenance fees. The current website is http://dor.sd.gov Information and access to the South Dakota Department of Revenue ("DOR") Intranet site will be provided during discovery.

1.2 ISSUING OFFICE AND RFP REFERENCE NUMBER

The Department of Revenue is the issuing office for this document and all subsequent addenda relating to it on behalf of the State of South Dakota, Department of Revenue. Unless the names of specific agencies are needed for clarity, the term "State" will be used in this RFP to refer to the DOR, the Bureau of Information and Telecommunications ("BIT"), both DOR and BIT, other selected State of South Dakota agencies or South Dakota state government as a whole. However, DOR will be the coordinating agency for all matters related to any Agreement resulting from this RFP. The reference number for the transaction is RFP #1274. This number must be referred to on all proposals, correspondence, and documentation relating to the RFP.

1.3 SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)

RFP Publication	February 1, 2018
Deadline for Submission of Written Inquiries	February 9, 2018
Responses to Offeror Questions	February 16, 2018
Proposal Submission	February 28, 2018
Oral Presentations/discussions (if required)	March 13-15, 2018
Proposal Revisions (if required)	March 19-20, 2018
Anticipated Award Decision/Contract Negotiation	March 23, 2018

.4 SUBMITTING YOUR PROPOSAL

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

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

An original and ten (10) identical copies of the proposal must be submitted.

The cost proposal must be in a separate sealed envelope and labeled "Cost Proposal".

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

REQUEST FOR PROPOSAL #1274
PROPOSAL DUE: February 28, 2018
BUYER Bobi Adams

SOUTH DAKOTA DEPARTMENT OF REVENUE

445 E CAPITOL AVE
PIERRE SOUTH DAKOTA 57501

All capital letters and no punctuation are used in the address. The address as displayed should be the only information in the address field.

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

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

By signing and submitting a proposal, the responder 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 responder is unable to certify to any of the statements in this certification, the responder will attach an explanation to its proposal.

1.6 NON-DISCRIMINATION STATEMENT

The State requires that all contractors, vendors, and suppliers doing business with the State to provide a statement of non-discrimination. By signing and submitting its proposal, the responder certifies it does not discriminate in its employment practices with regard to race, color, creed, religion, age, sex, ancestry, national origin, or disability.

1.7 MODIFICATION OR WITHDRAWAL OF PROPOSALS

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

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

1.8 RESPONDER INQUIRIES

Responders and their agents (including subcontractors, employees, consultants, or anyone acting on their behalf) may make written or email inquiries concerning this RFP to obtain clarification of requirements. No inquiries will be accepted after the date and time indicated in the section 1.3 Schedule of Activities. Email inquiries must be sent to Bobi Adams at Roberta.adams@state.sd.us with the subject line “RFP #1274”. If inquiries are submitted by mail, the envelope should be addressed to: Bobi Adams, South Dakota Department of Revenue, 445 E Capitol Ave., Pierre, South Dakota 57501. The RFP number should be included in the letter.

The DOR prefers to respond to responder’s inquiries (if required) via e-mail. If a responder does not indicate an email address, the DOR’S response will be sent via mail to the responder. All responders will be informed of any inquiries and the DOR’S response. Responders 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. Responders will be notified in the same manner as indicated above regarding any modifications to this RFP.

1.9 PROPRIETARY INFORMATION

The proposal of the successful responder 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. Responders must clearly identify in the Executive Summary and mark in the body of the proposal any specific proprietary information it is 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 DOR. All materials submitted become the property of the State and may be returned only at the State's option.

1.10 LENGTH OF CONTRACT

The estimated length of the contract is six (6) years. The first year would include programming and launch of the website, and the remaining five years would address maintenance.

1.11 **GOVERNING LAW**

Venue for any and all legal action regarding or arising out of the transaction covered under this RFP will be solely in the State of South Dakota. The laws of South Dakota, exclusive of its choice of law provisions, will govern this transaction.

1.12 **DISCUSSIONS WITH OFFERORS (ORAL PRESENTATION/NEGOTIATIONS)**

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

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

1.13 **FINANCIAL STATEMENTS**

A responder may be required to submit a copy of its most recent audited financial statement if deemed necessary by the State's Office of Procurement Management.

1.14 **BEST INTEREST OF SOUTH DAKOTA**

The DOR reserves the right to reject any or all proposals and may waive any immaterial deviation or defect in a proposal and make award(s) as deemed to be in the best interest of the State. The DOR's waiver of an immaterial deviation or defect will in no way modify the RFP or excuse the proposing responder from full compliance with the RFP requirements.

2.0 STANDARD CONTRACT TERMS AND CONDITIONS

Any contract or agreement resulting from this RFP will include the DOR'S standard terms and conditions as listed below, along with any additional terms and conditions as negotiated by the parties. A responder ("Consultant") should indicate in its response any concerns with the below terms. If no concerns are presented, the DOR assumes all terms are acceptable to the responder.

2.1 The Consultant will perform those services described in the Scope of Work, attached to the Agreement as Section 3 of the RFP and by this reference incorporated in the Agreement.

2.2 The Consultant's services under this Agreement will commence on April 1, 2017 and end on December 30, 2023, unless sooner terminated pursuant to the terms of the Agreement.

2.3 The Consultant will not use State equipment, supplies, or facilities. The Consultant will provide the State with its Employer Identification Number, Federal Tax Identification Number, or Social Security Number upon execution of this Agreement.

2.4 The State will make payment for services upon satisfactory completion of the services. The State will not pay Consultant's expenses as a separate item. Payment will be made pursuant to itemized invoices submitted with a signed state voucher. Payment will be made consistent with SDCL Ch. 5-26.

2.5 The Consultant will indemnify the State, its officers, agents, and employees against any and all actions, suits, damages, liability, or other proceedings that may arise as the result of performing services under the Agreement. 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.

2.6 The Consultant, at all times during the term of this Agreement, will obtain and maintain in full force insurance coverage of the types and with the limits as follows:

A. Commercial General Liability Insurance:

The Consultant will maintain occurrence based commercial general liability insurance or equivalent form with a limit of not less than $1,000,000.00 for each occurrence. If such insurance contains a general aggregate limit, it will apply separately to this Agreement or be no less than $2,000,000.00.

B. Professional Liability Insurance or Miscellaneous Professional Liability Insurance:

The Consultant will procure and maintain professional liability insurance or miscellaneous professional liability insurance with a limit not less than $1,000,000.00.

C. Business Automobile Liability Insurance:

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

D. Worker's Compensation Insurance:

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

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

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

No employee of the Contractor engaged in the performance of services required under this Agreement will be considered an employee of the State. No claim under the South Dakota Workers' Compensation Act on behalf of said employee or other person while so engaged and no claim made by any third party as a consequence of any act or omission of the part of the work or service provided or to be rendered under this Agreement by the Contractor will be the State's obligation or responsibility.

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

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

2.9 This Agreement may be terminated by the State upon thirty (30) days' written notice. This Agreement may be terminated by the Consultant for cause upon one hundred eighty (180) days' written notice. The Consultant is obligated to give the State one hundred eighty (180) days' written notice in the event the Consultant intends to not renew the Agreement or intends to raise any fees or costs associated with the Consultant's products or services in a subsequent contract. In the event the Consultant breaches any of the terms or conditions of the Agreement, the Agreement may be terminated by the State at any time with or without notice. Upon notice of termination or upon reaching the end of the term of the Agreement, and again at the effective date of the termination or end of the term, the State of South Dakota requires the Consultant to extract and provide to the State the State's information stored to repositories not hosted on the State's infrastructure. The information must be provided in a non-proprietary format that the State can

load onto/into the repositories listed in the State's standards. If the information cannot be extracted in a format that allows the information to be loaded onto or into the State's standard repositories the information (metadata [data structure descriptions] and data) will be extracted into a text file format and returned to the State. Upon termination, the State may take over the work and may award another party a contract to complete the work under this Agreement. In the event of termination or at the end of the term of this Agreement, the Consultant will deliver to the State all reports, plans, specifications, technical data, and all other information completed prior to the date of termination. If after the State terminates for a default by the Consultant it is determined that the Consultant was not at fault, then the Consultant will be paid for eligible services rendered and expenses incurred up to the date of termination. The Consultant recognizes and agrees that the State of South Dakota cannot enter into an agreement providing for hosting of any of its data on the Consultant's servers and networks without provisions protecting its ability to access and recover its data in a usable, non-proprietary format in the event of termination of this Agreement with sufficient time to convert that data and the business functions provided by the Consultant to another system and Consultant.

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

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

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

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

2.14 The Consultant may not use subcontractors to perform the services described herein without the express prior written consent of the State. 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.

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

2.16 Any notice or other communication required under this Agreement will be in writing and sent to the address set forth above. Notices will be given by and to Bobi Adams on behalf of the State, and by

_____, on behalf of 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 will be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination shall be sent by registered or certified mail, or, if personally delivered, when received by such party.

2.17 If any court of competent jurisdiction holds any provision of this Agreement unenforceable or invalid, such holding will not invalidate or render unenforceable any other provision of this Agreement. Failure to strictly enforce any provision of this Agreement will not operate as a waiver of any provision, right, or responsibility contained in this Agreement.

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

2.19 The Consultant will abide by all applicable provisions of the following assurances:

A. Title VI of the Civil Rights Act of 1964 (P.L. 88-352);
B. Title IX of the Education Amendments of 1972, as amended (20 U.S.C. §§ 1681-1683, and 1685-1686);
C. Section 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. §794) and the Americans with Disabilities Act of 1990 (42 USC § 12101, et seq.; PL 101-336);
D. Age Discrimination Act of 1975, as amended (42U.S.C. §§ 6101-6107);
E. Drug Abuse Office and Treatment Act of 1972 (P.L. 92-255), as amended;
F. Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970(P.L. 91-616), as amended;
G. Sections 523 and 527 of the Public Health Service Act of 1912 (42 U.S.C. §§ 290 dd-3 and 290 ee-3), as amended;
H. Title VIII of the Civil Rights Act of 1968 (42 U.S.C. §§ 3601 et seq);
I. Civil Rights Restoration Act of 1987;
J. Drug-free Workplace Act of 1988 (41 U.S.C. 702);
K. Buy America Act (49 U.S.C. 5323 (j));
L. Hatch Act (5 U.S.C. §§ 1501-1508 and 7324-7328);
M. Executive Order 11246 Equal Employment Opportunity;
N. Contract Work Hours and Safety Standards Act (40 U.S.C. §§ 3701-3708);
O. Clean Air Act (42 U.S.C. §§ 7401-7671q) and the Federal Water Pollution Control Act (33 U.S.C. §§ 1251-1387);
P. Debarment and Suspension (Executive Orders 12549 and 12689); and
Q. Byrd Anti-Lobbying Amendment (31 U.S.C. § 1352).

2.20 The Consultant will maintain or supervise the maintenance of records necessary for the proper and efficient operation of the program, including records and documents regarding applications, determination for 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 will retain such records for six (6) years following termination of this agreement. If such records are under pending audit, the Consultant will 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.

2.21 Automatic upgrades to any software used by the Consultant to provide any services that simply improve the speed, efficiency, reliability, or availability of existing services and do not alter or add functionality are not considered “changes to the Services,” and such upgrades will be implemented by the Consultant on a schedule no less favorable than that provided by the Consultant to any other customer receiving comparable levels of services

2.22 The Consultant will be responsible for the professional quality, technical accuracy, timely completion and coordination of all services furnished by the Consultant and any subcontractors, if applicable, under this Agreement. The Consultant will, without additional compensation, correct or revise any errors or omissions in its work products.

The following clauses pertain to technical, data and security issue. Any contract or agreement resulting from this RFP will include the DOR’S standard terms and conditions as listed below, along with any additional terms and conditions as

negotiated by the parties. A responder (“Consultant”) should indicate in its response any concerns with the below terms. If no concerns are presented, the DOR assumes all terms are acceptable to the responder.

2.23 **Work Product**

The Consultant shall be responsible for the professional quality, technical accuracy, timely completion, and coordination of all services furnished by the Consultant and any subcontractors, if applicable, under this Agreement. It shall be the duty of the Consultant to assure that the services and the system are technically sound and in conformance with all pertinent Federal, State and local statutes, codes, ordinances, resolutions and other regulations. The Consultant shall, without additional compensation, correct or revise any errors or omissions in its work products.

Consultant hereby acknowledges and agrees that all reports, plans, specifications, technical data, miscellaneous drawings, agreements, State Proprietary Information, any information discovered by the State, End User Data, Personally Identifiable Information (PII), data protected under Family Educational Rights and Privacy Act (FERPA), Personal Heath Information (PHI), Federal Tax Information (FTI) or any information defined under state statute as confidential, and all information contained therein provided to the State by the Consultant in connection with its performance 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.

Papers, reports, forms or other material which are a part of the work under this Agreement will not be copyrighted without written approval of the State. In the event that any copyright does not fully belong to the State, the State reserves a royalty-free, non-exclusive, non-transferable and irrevocable license to reproduce, publish, and otherwise use and to authorize others to use on the State's behalf any such work for government purposes.

2.24 **Source Code**

Consultant hereby agrees to provide to the South Dakota Bureau of Information and Telecommunications, for safekeeping, a copy of source code developed or maintained for use by the State under the terms of this agreement. The source code provided will be the version currently running on the State's production environment

2.25 **Domain Name Ownership**

Any website(s) that the Consultant creates as part of this project must have the domain name registered by and owned by the State. If as part of this project the Consultant is providing a service that utilizes a website with the domain name owned by the Consultant, the Consultant must give thirty (30) days' notice before abandoning the site. If the Consultant intends to sell the site to another party the Consultant must give the State thirty days (30) notice and grant the State the right of first refusal. For any site or domain, whether hosted by the Consultant or within the State web infrastructure, any and all new web content should first be created in a development environment and then subjected to security scan before being approved for a move up to the production level.

2.26 **Information Technology STANDARDS**

Any software or hardware provided under this agreement will comply with state standards which can be found at http://bit.sd.gov/standards/ . Consultants should especially take note of the web standards found at http://bit.sd.gov/standards/web.aspx.

2.27 **Browser**

The system, site, and/or application must be compatible with the State's current browser standard which can be found at http://bit.sd.gov/standards/ BIT standards are inclusive Explorer 11 and Microsoft Edge. QuickTime, PHP, and Adobe ColdFusion, Adobe Flash or Adobe Animate CC will not be used in the system, site, and/or application.

2.28 **Acceptable Programming Languages**

The application(s) covered in this contract will be written in C#.NET, ASP.NET, or VB.NET.

2.29 **License Agreements**

Consultant warrants that it has provided to the State and incorporated into this agreement all license agreements, End User License Agreements, and terms of use regarding its software or any software incorporated into its software before execution of this agreement. Failure to provide all such license agreements, End User License Agreements, and terms of use shall be a breach of this agreement at the option of the State. The parties agree that neither the State nor its end users shall be bound by the terms of any such agreements not timely provided pursuant to this paragraph and incorporated into this

Agreement. Consultant agrees that it shall indemnify and hold the State harmless from any and all damages or other detriment, actions, lawsuits or other proceedings that arise from failure to provide all such license agreements, End User License Agreements, and terms of use or that arise from any failure to give the State notice of all such license agreements, End User License Agreements, and terms of use. Any changes to the terms of this Agreement or any additions or subtractions must first be agreed to by both parties in writing before they go into effect. This paragraph shall control and supersede the language of any such agreements to the contrary.

2.30 **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 known security issues are resolved.

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. This investigation can include security scans made at the State's discretion.

C. State technology standards, policies, and best practices will be followed. State technology standards can be found at http://bit.sd.gov/standards/.

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

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

F. State access to the source code will be allowed to ensure State security standards, policies, and best practices which can be found at http://bit.sd.gov/standards/.

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

i. The previous version of the third party code base or platform is no longer being maintained, patched, and supported; and

ii. The new version to which the State moved the application is actively maintained, patched, and supported.

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

If a code base or platform on which the Consultant's application depends is no longer supported, maintained, or patched by a qualified third party the Consultant commits to migrate its application from that code base and/or platform to one that is supported, maintained, and patched after the State has performed a risk assessment using industry standard tools and methods. Based on that assessment, the Consultant will fix or mitigate the risk based on the following schedule: high risk, within 7 days, medium risk within 14 days, low risk, within 30 days. Failure on the part of the Consultant to work in good faith with the State toward a timely move to supported, maintained, and patched technology will allow the State to cancel this Agreement without penalty.

2.31 **Security Acknowledgement Form**

The Consultant will be required to sign the Security Acknowledgement form which is attached to this Agreement as Appendix B. 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- Contractor (ITSP), provided on request. 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.

2.32 **Background Checks**

The State of South Dakota requires all employee(s) of the Consultant, Subcontractor's, Agents, Assigns and or Affiliated Entities who write or modify State of South Dakota-owned software, alter hardware, configure software of state-owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas to undergo fingerprint-based background checks. These background checks must be performed by the State with support from the State's law enforcement resources. The State will supply the finger print cards and prescribe the procedure to be used to process the finger print cards. Project plans should allow two to four 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 of South Dakota owned software, altering hardware, configuring software of state owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas then, background checks must be performed on any employees who will complete any of the referenced tasks. The State reserves the right to require the Consultant to prohibit any employee, Subcontractor's, Agents, Assigns and or Affiliated Entities from performing work under this Agreement that the State, in its sole discretion, believes 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 its determination.

2.33 **Security Incident and Breach Notification**

The Consultant, unless stipulated otherwise, shall notify the State Contact within 12 hours if the Consultant reasonably believes there has been a security incident.

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

2.34 **Threat Notification**

Upon becoming aware of a possible security threat(s) or exploit(s) with the Consultant's product(s) and or service(s) being used by the State the Consultant will notify the State within to (2) business days of any such threat(s) or exploit(s) and, if the State requests, provide the State with information on the threat(s) or exploit(s).

2.35 **Handling of Data Breaches**

The Consultant will implement, maintain and update security incident and data breach procedures that comply with all State standards and Federal requirements. A data breach is the disclosure of, unauthorized access to, or use of, or modification of, or destruction of State data or the interference with system operations in an information system containing State data. 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 data breach, including any post-incident review of events and actions taken to implement changes in business practices in providing the services covered by this agreement.

The Consultant will preserve all evidence including but not limited to communications, documents, and logs and the State will have the authority to set the scope of the investigation. In addition, the Consultant shall inform the State of actions being taken or will be taken to reduce the risk of further loss to the State

2.36 **Curing of Breach of Agreement**

In the event of a breach of these representations and warranties the State may, at the State's discretion, provide the Consultant with the opportunity to rectify the breach. The Consultant shall immediately, after

notice from the State, begin work on curing such breaches. If the notice is telephonic the State will provide, at the Consultant's request, a written notice to reaffirm the telephonic notice. If such problem remains unresolved after three days, at State's discretion, Consultant will send, at Consultant's sole expense, at least one qualified and knowledgeable representative to the State's site where the system is located. This representative will continue to address and work to remedy the deficiency, failure, malfunction, defect, or problem at the site. The rights and remedies provided in this paragraph are in addition to any other rights or remedies provided in this Agreement or by law.

2.37 **Security Scanning**

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

2.38 **WEB AND Mobile Applications**

The Consultant's application is required to;

A. have no code or services including web services included in or called by the application unless they provide direct, functional requirements that support the State's business goals for the application;
B. encrypt data in transport and at rest using a mutually agreed upon encryption format;
C. close all connections and close the application at the end of processing;
D. The documentation will be in grammatically complete text for each call and defined variables (No abbreviations and use complete sentences, for example)sufficient for a native speaker of English with average programming skills to determine the meaning and or intent of what is written without having prior knowledge of the application.
E. have no code not required for the functioning of application;
F. have no "back doors", a back door being a means of accessing a computer program that bypasses security mechanisms, or other entries into the application other than those approved by the State;
G. permit no tracking of device user's activities without providing a clear notice to the device user and requiring the device user's active approval before the application captures tracking data;
H. have no connections to any service not required by the functional requirements of the application or defined in the project requirements documentation;
I. fully disclose in the "about" information that is the listing of version information and legal notices, of the connections made, permission(s) required, and the purpose of those connections and permission(s);
J. ask only for those permissions and access rights on the user's device that are required for the defined requirements of the Consultant's application;
K. access no data outside that which is defined in the "About" information for the Consultant's application;

The Consultant is required to disclose all:

A. functionality;
B. device and functional dependencies; and
C. third party libraries used. (or ; if the rest if the red text is used)

2.39 **Product Conformity**

The State has twelve (12) months following final acceptance of the product(s) delivered by the Consultant pursuant to this Agreement to verify that the product(s) conform to the requirements of this Agreement and perform according to the Consultant's system design specifications. Upon the State's recognition of an error, deficiency, or defect, the Consultant shall be notified by the State. The notification shall cite any specific deficiency (deficiency being defined as the Consultant having performed incorrectly with the information previously provided by the State, not the Consultant having to modify a previous action due to additional and/or corrected information from the State). The Consultant, at no additional charge to the State, shall provide a correction or provide a mutually acceptable plan for correction within thirty-days following the receipt of the State's notice to the Consultant. If the Consultant's correction is inadequate to correct the deficiency, or defect, or if error recurs, the State may, at its option, act to correct the problem. The Consultant shall be required to reimburse the State for any such costs incurred or the State will consider this to be a breach of the agreement. Payment by the Consultant pursuant to this provision does not waive any other rights and remedies available to the State.

2.40 **Product Installation and Operation**

The State will install and operate the Consultant's product on the State's computing infrastructure. The State's installation process and operation of the product will follow current State standards which can be found at http://bit.sd.gov/standards/. It is the Consultant's responsibility to review these standards and alert the state if the costs enumerated in the agreement will change based on State standards. The State will not be responsible for added licensing or processing costs if the Consultant determines at a later date, that by following the standards in effect at the time of installation the State is or would be obligated to pay fines, additional rates, fees, license costs or charges of any type, additional charges of any type or character for Consultant's or a third party's intellectual property, or added support costs

2.41 **Denial of Access or Removal of an Application from Production**

During the life of this agreement the application can be denied access to or removed from production at the State's discretion. The reasons for the denial of access or removal of the application from the production system may include security, functionality, unsupported third party technologies, or excessive resource consumption of resources. The Consultant will be liable for additional work required to rectify issues concerning security, functionality, unsupported third party technologies, and or excessive consumption of resources if it is for reasons of correcting security deficiencies or meeting the functional requirements originally agreed to for the application. At the discretion of the State, contractual payments may be suspended while the application is denied access to or removed from production if the problem is caused by the Consultant's actions or inactions. Access to production and any updates to production will be made only with the State's prior approval. It is expected that the Consultant shall provide the State with proof of the remedy proposed before the State provides access to production. The State shall sign a non-disclosure agreement with the Consultant if revealing the remedy will put the Consultant's intellectual property at risk. If the Consultant is unable to produce the project deliverables due to the Consultant actions or inactions within thirty (30) days of the application's denial of access or removal from production and the Consultant does not employ the change management process to alter the project schedule or deliverables within the same thirty (30) days then at the State's discretion the agreement may be terminated.

.42 **Movement of Product**

The State operates a virtualized computing environment and retains the right to use industry standard hypervisor high availability, fail-over, and disaster recovery systems to move instances of the product(s) between the install sites defined with the Consultant within the provisions of resource and usage restrictions outlined elsewhere in the agreement. As part of normal operations the State may also install the product on different computers or servers if the product is also removed from the previous computer or server within the provisions of resource and

usage restrictions outlined elsewhere in the agreement. All such movement of product can be done by the State without any additional fees or charges by the Consultant.

.43 **Use of product on virtualized infrastructure and changes to that infrastructure**

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

.44 **Load Balancing**

The State routinely load balances across multiple servers applications that run on the State's computing environment. The Consultant's product must be able to be load balanced across

multiple servers. Any changes or modifications required to allow the Consultant's product to be load balanced so that it can operate on the State's computing environment will be at the Consultant's expense.

.45 **Use of Abstraction Technologies**

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

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

3 SCOPE OF WORK

The responder will design, code, and populate a responsive internet website for all normal and mobile applications. The responder will be required to work with the Bureau of Information and Telecommunications (BIT) to meet its technology and security requirements in all stages (as referenced in this RFP). In addition they will work with BIT to integrate their design into the State's content management system (CMS) to populate all current and new content. Also the Responder will work with BIT to oversee the launch of and troubleshoot the website rollout. The responder will provide maintenance on the websites for a minimum of five (5) years. The site will remain hosted by the State and not off-site.

South Dakota Department of Revenue Overview

The South Dakota Department of Revenue (DOR) is a state agency that serves the citizens, businesses and governmental entities of South Dakota through a variety of divisions. The focus of our department is to serve South Dakotans and to support government services by collecting all taxes required by law, supporting motor vehicle requirements, and regulating the gaming industry and state's lottery to raise revenue for government programs. This is accomplished by providing taxpayers with current and complete information, education programs, and up-to-date technology to support tax filings, payments and motor vehicle registration. Our efforts have yielded high voluntary compliance rates in all areas and have promoted commitment, communication, and customer service.

We recognize our responsibilities to our customers, and service is a priority. We are pleased to offer our professional services through the Internet and will continue to make progress while always promoting efficiency.

Our Audience – Internet (http://dor.sd.gov/)

The primary audience of the DOR's external website is employees, local, state, tribal and federal government agencies; consultants; legislators; and the general public.

Current Website

The current website, dor.sd.gov, is about seven (7) years old and does not serve internal or external customers as well as it could. The design needs to better reflect our brand, educate and inform, have more intuitive navigation and updated content. Overall, the website lacks a clear path for our visitors and employees to follow to find what they want in order to do business with us.

New Website Objectives and Deliverables:

Each numbered section below should be broken down individually for both hours and cost in the response.

1. Content evaluation, development, enhancement
    a. Search other state DOR's websites for ideas related to design and additional content
        i. DOR sites from Iowa, Ohio, Washington and Minnesota are examples for both website functionality and expanded content for both internal and external use.
    b. Use Google Analytics, internal and external survey's (noted in 1.c.) to analyze the current site to determine what pages are not getting used and see if they should be eliminated, combined with other information or relocated.
    c. Survey employees, partners, customers and the general public on the current website for items such as aesthetics, ease of use, navigation, intuitiveness, etc.
    d. Provide creative, time-saving solutions that may include automation by connecting to databases, populating page links automatically when files are added to a folder, outlook calendar linking, etc. to provide up-to-date information by a variety of people using the CMS. The goal of this is to allow more people to update some information to improve content and timeliness of content.
    e. Re-evaluate content and structure with follow-up surveys and Google Analytics evaluation after one year of use to see if the changes have been effective and suggest modifications
    f. Follow up with surveys and Google Analytics to see how the website is working and make changes accordingly to best serve employees and the customer.

2. Structure and Design.

3. Populate content for all pages using a CMS system designed by the State of South Dakota Bureau of Information and Telecommunications.

4. Maintenance for 5 years.

5. Info-graphics and social media posts for 6 months to promote the new website and the new logo through press and social media (no budget for paid advertising).

New Website Requirements

The new website will inform and educate, engage our customer base, and position our brand as a leader through resource content and streamlined design.

- Move away from the "old and stodgy" government agency look and feel and move to an agency that is transparent, responsive, engaged, forward-thinking, strategic, technologically advanced, fiscally responsible and beneficial to the communities we reside in.
- The website must comply with state standards which can be found at http://bit.sd.gov/standards/
- Intuitive Navigation
- Website must interact with our applications. Some applications must look as though they reside within the website. In the future, DOR also wants the ability to publish Business Intelligence reports (i.e. Microsoft Power BI, Table9au) from our site.
- Clean, focused and responsive design
- Meet all federal information technology standards and web accessibility guidelines.
- Updated, relevant and informative content that is clear and concise about what we do and what we don't do (i.e. driver licensing, motor carrier, motor vehicle)
- SEO optimization – we are not looking for rankings, but proper SEO for businesses/customers.
- Social media integration
- **Browser (Section 2.27 above)**
- The system, site, and/or application must be compatible with supported versions of Edge, Chrome, Safari, Firefox and Internet Explorer browsers. QuickTime, PHP, Adobe ColdFusion, Adobe Flash and Adobe Animate CC will not be used in the system, site, and/or application.
- **Acceptable Programming Languages (Section 2.28 above)**
  The system, site, and/or application must be compatible with supported versions of Edge, Chrome, Safari, Firefox and Internet Explorer browsers. QuickTime, PHP, Adobe ColdFusion, Adobe Flash and Adobe Animate CC will not be used in the system, site, and/or application.

Website Option Considerations:

While not required to be part of the website, DOR is interested in exploring these options on a new website.

- Multilingual accessibility or translation.
- Vendor built CMS
- Creation of user generated web forms with user generated content
- Would consider Responder hosting option based on security and support response time

Website Maintenance

The website will be a joint effort between the Responder, BIT and DOR. For ongoing maintenance DOR would want Responder to troubleshoot problems and assist BIT and / or DOR with design elements and maintaining the navigation, SEO elements and social media integration.

4 PROPOSAL REQUIREMENTS AND COMPANY QUALIFICATIONS

4.1 The responder is cautioned that it is the responder'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**: Responders and their agents (including subcontractors, employees, consultants, or anyone else acting on their behalf) must direct all of their questions or comments regarding the RFP and the evaluation to the buyer of record indicated on the first page of this RFP. Responders 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 or exclusion from specific procurements. Responders and their agents who have questions regarding this matter should contact the buyer of record.

4.3 The responder may be required to submit a copy of its most recent audited financial statements upon the State's request.

4.4 The responder should provide the following information related to at least three (3) previous and current service/contracts, performed by the responder's organization, which are similar to the requirements of this RFP. Responders should also provide this information for any service/contract that has been terminated, expired or not renewed in the past three (3) years.

4.4.1 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;

4.4.2 Dates of the service/contract; and

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

5 PROPOSAL RESPONSE FORMAT

5.1 An original and ten (10) copies shall be submitted.

5.1.1 In addition, the offeror should provide one (1) copy of its entire proposal, including all attachments, in Microsoft Word or PDF electronic format. Due to security concerns the State

will not accept electronic proposals on portable media so Offerors must provide a secure location where the State can electronically download the Offeror's proposal(s). This secure location can be a SFTP site, an encrypted FTP site or a webpage using SSL if files are only downloaded and nothing has to be uploaded. Offeror's shall reference their secure web location in the paper copy of their proposal.

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

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

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

5.2.2 **Executive Summary.** The one or two page executive summary is to briefly describe the responder'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 responder's assessment of the work to be performed, the responder's ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the offeror's understanding of the desired overall performance expectations.

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

5.2.3.3 A clear description of any options or alternatives proposed.

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

5.2.5 **Cost Proposal.** Responders may submit multiple cost proposals. The State requires at least two cost (2) proposals: one providing the costs if the responder hosts the website and one providing the costs if the State hosts the website. All costs related to the provision of the required services must be included in each cost proposal offered.

5.2.5.1 **Format of Cost Proposal**
The Responder should break their costs down into the 6 areas as noted under Section 3 – Scope of Work.

6 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) will use subjective judgment in conducting a comparative assessment of the proposal by considering each of the following criteria:

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

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

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

6.1.4 Availability to the project locale;

6.1.5 Familiarity with the project locale;

6.1.6 Proposed project management techniques; and

6.1.7 Ability and proven history in handling special project constraints.

6.2 Experience and reliability of the responder's organization are considered subjectively in the evaluation process. Therefore, the responder 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 responder to perform the requirements of this RFP, whether from the responder's organization or from a proposed subcontractor, will be subjectively evaluated. Therefore, the responder 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 responder will mutually discuss and refine the scope of services for the project and will negotiate terms, including compensation and performance schedule.

6.5.1 If the agency and the highest ranked responder 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 responder. The agency may then negotiate with the next highest ranked responder.

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.

7.0 TECHNOLOGY QUESTIONS

Any contract or agreement resulting from this RFP will include the State's standard I/T contract terms listed in Appendix A, along with any additional contract terms as negotiated by the parties. As part of the negotiation process the contract

terms listed within the RFP and Appendix B may be altered or deleted. The Offeror should indicate in their response any issues they have with specific contract terms if the Offeror does not that there are any issues with any contract terms then the State will assume those are acceptable to the Offeror.

See Appendix A and B

Appendix A 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 _____ Employee's BIT Manager _____ Date _____

Employee or Contractor name and Company name in block capital letters _____

Revised September 2016 Page | 1

Appendix B Security and Vendor Questions

For the vendor the following questions are used by the Bureau of Information and Telecommunications to determine if your company's policies and procedures are a good fit with the State of South Dakota. Not all questions will apply and you may answer Not Applicable. Please note that many questions require additional explanation based on your answer.

A = Data Center B = Developmen t C = PMO Office D = Telecommunications

	BIT Owner	Question	Response	Add text as required
1.	C	Typically the State of South Dakota prefers to host all systems. In the event that the State decides that it would be preferable for the vendor to	Yes☐ No☐ NA ☐	
2.	D	Is there a workstation install requirement?	Yes☐ No☐ NA ☐	
3.	A/ D	Is this a browser based User Interface?	Yes☐ No☐ NA ☐	
4.	B/ C	What is the development technologies used for this system? ASP _____ VB.Net _____ C#.Net _____ .NET Framework _____		
5.	A	clues about valid username or password content or structure, for example when a user forgets their username or after a failed login attempt? Are usernames and passwords generated by the system using user-specific information such as last name or birthdate? If Yes to these,	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
6.		Is a user required to change their password? How often? What are the complexity requirements for the passwords? (BIT password requirements are available in Section 230.67.4.4 of the Information	Yes☐ No☐ NA ☐	
7.	A	Will the system infrastructure require an email interface?	Yes☐ No☐ NA ☐	
8.	A	Will the system require a database?	Yes☐ No☐ NA ☐	
9.	A	Will the system infrastructure require database replication?	Yes☐ No☐ NA ☐	

10.	A	Will the system require transaction logging for database recovery?	Yes☐ No☐ NA ☐	
11.	A	Will the system infrastructure have a special backup requirement?	Yes☐ No☐ NA ☐	

12.	A	If your application is hosted on the state's infrastructure will it require a dedicated environment?	Yes☐ No☐ NA ☐	
13.	A	If your application is hosted on a dedicated environment within the state's infrastructure are all costs for the needed software licenses included in your cost proposal? If so will you provide copies of the licenses with a line-item list of their proposed costs	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
14.	A	If your application is running on a dedicated environment on the state's infrastructure and there is additional software licenses covered in your proposal will these licenses be in the state's name? If not, please explain	Yes☐ No☐ NA ☐	
15.	B/ C	Will the system provide an archival solution? If not is the State expected to develop a customized archival	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
16.	A	Will the system infrastructure have any processes that require	Yes☐ No☐ NA ☐	
17.	A/ B	Will the system infrastructure include a separate OLTP or Data Warehouse Implementation?	Yes☐ No☐ NA ☐	
18.	A/ B	Will the system infrastructure require a Business Intelligence solution?	Yes☐ No☐ NA ☐	
19.	B/ C	Will the system have any workflow requirements?	Yes☐ No☐ NA ☐	
20.	C	Explain the software licensing model.	Yes☐ No☐ NA ☐	
21.	A	If the product is hosted at the state will there be a request to include an application to monitor license compliance?		
22.	A	The State expects to be able to move your product without cost for Disaster Recovery purposes and to maintain high availability. Will this	Yes☐ No☐ NA ☐	
23.	A	Can the system be implemented via Citrix?	Yes☐ No☐ NA ☐	
24.	B/ D	Will the system implement its own level of security?	Yes☐ No☐ NA ☐	
25.	A	Can the system be integrated with our enterprise Active Directory to ensure access is controlled?	Yes☐ No☐ NA ☐	
26.	A	Will the system print to a Citrix compatible networked printer?	Yes☐ No☐ NA ☐	
27.	D	Will the network communications meet IEEE standard TCP/IP and use either standard ports or State defined ports	Yes☐ No☐ NA ☐	

28.	A/ D	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)?	Yes☐ No☐ NA ☐	

29.	D	Will the system provide Internet security functionality on a public portal to include firewalls?	Yes☐ No☐ NA ☐	
30.	D	It is State policy that no equipment can be connected to State Network without direct approval of BIT Network Technologies, would this affect the	Yes☐ No☐ NA ☐	
31.	D	Does your application use Java, is it locked into a certain version or will it use the latest version if so what is your process for updating the application?	Yes☐ No☐ NA ☐	
32.	D	If your application does not run under the latest Microsoft operating system what is your process for updating the		
33.	A	Will the server based software support: a. Windows server 2012 R2 b. IIS7.0 or higher c. MS SQL Server 2008R2 or higher d. Exchange 2010 or higher e. Citrix presentation server 4.5 or higher f. VMWare ESXi 5.5 or higher g. MS Windows Updates h. Symantec End Point Protection	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
34.	B	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		
35.	D	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	Yes☐ No☐ NA ☐	
36.	A	It is State policy that all systems must be compatible with BITs dynamic IP addressing solution (DHCP). Would this affect the implementation of the	Yes☐ No☐ NA ☐	
37.	A	It is State policy that all systems that require an email interface must leverage existing SMTP processes currently managed by BIT Datacenter. Mail Marshal is the existing product used for SMTP relay. Would this affect	Yes☐ No☐ NA ☐	
38.	D	It is State policy that all Vendor/Contractor Remote Access to systems for support and maintenance on the State Network will only be allowed through Citrix Secure Gateway. Would this affect the implementation	Yes☐ No☐ NA ☐	
39.	D	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	Yes☐ No☐ NA ☐	

40.	A	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. If need is determined by the State, would this affect the	Yes☐ No☐ NA ☐	
41.	A	The State has a virtualize first policy that requires all new systems to be configured as virtual machines. Would this affect the implementation	Yes☐ No☐ NA ☐	
42.	D	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	Yes☐ No☐ NA ☐	
43.	D	It is State policy that systems must support NAT and PAT running inside the State Network. Would this affect the implementation of the system?	Yes☐ No☐ NA ☐	
44.	D	It is State policy that systems must not use dynamic TCP or 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	Yes☐ No☐ NA ☐	
45.	D	Will your system use Adobe Air, Adobe Flash, Apache Flex, JavaFX, Microsoft Silverlight or QuickTime? If yes what are your plans for moving off them?	Yes☐ No☐ NA ☐	
46.	D	Does your web application use PHP or Adobe ColdFusion?	Yes☐ No☐ NA ☐	
47.	A/ B	How does data enter the system (transactional or batch or both)?		
48.	C	Is the system data exportable by the user for use in tools like Excel or	Yes☐ No☐ NA ☐	
49.	C	Will user customizable data elements be exportable also?	Yes☐ No☐ NA ☐	
50.	C	Will the system distinguish between local versus global administrators where local administrators have rights to user management only for the program area that they are associated with and global administrators have rights for the	Yes☐ No☐ NA ☐	
51.	C	Will this system provide the capability to track data entry/access by the person, date and time?	Yes☐ No☐ NA ☐	
52.		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	Yes☐ No☐ NA ☐	

53.	A/ B/ C/	Will the system provide data encryption for sensitive information both in storage and transmission?	Yes☐ No☐ NA ☐	
	D			
54.		Are account credentials hashed and encrypted when stored?	Yes☐ No☐ NA ☐	
55.	D	It is State policy that systems at the discretion of the State may be scanned by BIT or a 3rd Party for security vulnerabilities. Scanning could take place annually as well as	Yes☐ No☐ NA ☐	
56.	C/ D	The Vendors/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 vendor's answers to the follow-up questions may be required in writing and/or verbally. The answers provided	Yes☐ No☐ NA ☐	
57.	A	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.	Yes☐ No☐ NA ☐	
58.	A/ C	Will the vendor provide assistance with installation?	Yes☐ No☐ NA ☐	
59.	A/ C	Is there an installation guide available and will you provide a copy to the	Yes☐ No☐ NA ☐	
60.	A/ C	Is telephone assistance available for both installation and use?	Yes☐ No☐ NA ☐	
61.	A/ B /C	Is on-site assistance available? If so, is there a charge?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
62.	A/ B /C	Will the implementation plan include user acceptance testing?	Yes☐ No☐ NA ☐	
63.	A/ B /C	Will the implementation plan include performance testing?	Yes☐ No☐ NA ☐	
64.	A	Will SSL traffic be decrypted and inspected?	Yes☐ No☐ NA ☐	
65.	B	Will technical documentation for application maintenance purposes be provided to the State?	Yes☐ No☐ NA ☐	
66.	B/ C	Will there be documented test cases for future releases including any customizations done for the State of	Yes☐ No☐ NA ☐	
67.	C	Can the user manual be printed?	Yes☐ No☐ NA ☐	
68.	C	Is the user manual electronically available?	Yes☐ No☐ NA ☐	

69.	C	Is there on-line help assistance available?	Yes☐ No☐ NA ☐	
70.	C	Describe your Support options.		
71.	A/C	Is there a method established to communicate availability of system	Yes☐ No☐ NA ☐	
72.	A/D	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 in regards to	Yes☐ No☐ NA ☐	
73.	B/C	Will you provide customization of the system if required by the State of South Dakota?	Yes☐ No☐ NA ☐	
74.	B	Will the state be required to develop customized interfaces to other	Yes☐ No☐ NA ☐	
75.	B	Will the State be required to develop reports or data extractions from the database?	Yes☐ No☐ NA ☐	
76.	A/B/C	Will the State of South Dakota have access to the underlying data and data model for ad hoc reporting purposes?	Yes☐ No☐ NA ☐	
77.	C	Will the source code for the system be put in escrow for the State of South Dakota?	Yes☐ No☐ NA ☐	
78.	C	If the source code is placed in escrow, will the vendor pay the associated escrow fees?	Yes☐ No☐ NA ☐	
79.	B/C	If the State of South Dakota will gain ownership of the software, does the proposal include a knowledge	Yes☐ No☐ NA ☐	
80.	C	Explain the basis on which pricing could change for the state based on your licensing model.		
81.	C	Contractually, how many years price lock are you offering the state as part of your response? Also as part of your response, how many additional years are you offering to limit price increases		
82.	B/C	Has your company ever integrated this product with an enterprise service bus to exchange data between diverse computing	Yes☐ No☐ NA ☐	
83.	B/C	Has your company ever conducted a project where you were tasked with performing load testing?	Yes☐ No☐ NA ☐	
84.	B/C	system that ran on Citrix Metaframe?	Yes☐ No☐ NA ☐	
85.	B/C	Have you ever created a User Acceptance Test plan and test cases?	Yes☐ No☐ NA ☐	
86.	C	It is State policy that all Vendor/Contractor Remote Access to systems for support and maintenance on the State Network will only be allowed through Citrix Secure Gateway or Skype for Business. Would this affect	Yes☐ No☐ NA ☐	

87.	C	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. Vendor should specify what access requirements are for user access to the system and what requirements are for any system level processes. Vendor should describe all requirements in		
88.	C	Are there expected periods of time where the application will be unavailable for use?	Yes☐ No☐ NA ☐	
89.	C	Is there a strategy for mitigating unplanned disruptions?	Yes☐ No☐ NA ☐	
90.	C	Will the State of South Dakota own the data created in your hosting	Yes☐ No☐ NA ☐	
91.	C	Will the State acquire the data at contract conclusion?	Yes☐ No☐ NA ☐	
92.	C	Will organizations other than the State of South Dakota have access	Yes☐ No☐ NA ☐	
93.	C	Will the State's data be used for any other purposes other than South Dakota's usage?	Yes☐ No☐ NA ☐	
94.	C	Will the State's data be protected?	Yes☐ No☐ NA ☐	
95.	C	propose to use that is not state standard, the standards can be found at http://bit.sd.gov/standards/.		
96.	A	Please explain the pedigree of the software, include in your answer who are the people, organization and processes that created the		
97.	A	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		
98.	D	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	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
99.	B	What are the processes (e.g., ISO 9000, CMMi), methods, tools (e.g., IDEs, compilers) techniques, etc. used to produce and transform the software		
100.	B	Explain the use cases used for software assurance during		

101.	D	Describe the training your company offers related to defining security requirements, secure architecture and design, secure coding practices, and		
102.	D	Do you have developers that possess software security related certifications (e.g., the SANS secure coding	Yes☐ No☐ NA ☐	
103.	B	Does your company have a policy and process for supporting/requiring professional certifications? If so, how do you ensure certifications are valid	Yes☐ No☐ NA ☐	
104.	B	Are there some requirements for security that are “structured” as part of general releasability of a product and others that are “as needed” or	Yes☐ No☐ NA ☐	
105.	D	What process is utilized by your company to prioritize security related enhancement requests?		
106.	D	What threat assumptions were made, if any, when designing protections for the software and information		
107.	D	In preparation for release, are undocumented functions in the software disabled, test/debug code removed, and source code comments	Yes☐ No☐ NA ☐	
108.	A	Explain how and where the software validates (e.g., filter with white listing) inputs from untrusted sources before		
109.	D	Has the software been designed to execute within a constrained execution environment (e.g., virtual machine, sandbox, chroot jail, single-purpose pseudo-user) and is it designed to isolate and minimize the extent of	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
110.	D	Where applicable, does the program use run- time infrastructure defenses (such as address space randomization, stack overflow protection, preventing execution from	Yes☐ No☐ NA ☐	
111.	D	How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques		
112.	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)? If so, please list those third	Yes☐ No☐ NA ☐	
113.	D	What security criteria, if any, are considered when selecting third-		
114.	B	What coding and/or API standards are used during development of the		
115.	B	What types of functional tests are/were performed on the software during its development (e.g., spot checking, component- level testing		

116.	D	Who and when are security tests performed on the product? Are tests performed by an internal test team, by an independent third party, or by both?		
117.	B	Are misuse test cases included to exercise potential abuse scenarios of the software?	Yes☐ No☐ NA ☐	
118.	B	Are security-specific regression tests performed during the development process? If yes, how frequently are the tests performed?	Yes☐ No☐ NA ☐	
119.	D	What release criteria does your company have for its products with regard to security?		
120.	B	What controls are in place to ensure that only the accepted/released software is placed on media for		
121.	B	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		
122.	D	How has the software been measured/assessed for its resistance to identified, relevant attack patterns? Are Common Vulnerabilities & Exposures (CVE®) or Common Weakness Enumerations (CWEs) used?		
123.	D	Has the software been evaluated against the Common Criteria, FIPS 140-2, or other formal evaluation process? If the CC, what evaluation assurance level (EAL) was achieved? If the product claims conformance to a protection profile, which one(s)? Are	Yes☐ No☐ NA ☐	
124.	A/D	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? performed? Are SwA experts involved	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
125.	A/B	Does the software contain third-party developed components? If yes, are those components scanned by a static code analysis tool?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
126.	A/D	Has the product undergone any penetration testing? When? By whom? Are the test reports available under a nondisclosure agreement? How have the findings been mitigated?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	

127.	B	Are there current publicly-known vulnerabilities in the software (e.g., an unrepaired CWE entry)? If yes please explain.	Yes☐ No☐ NA ☐	
128.	A/B	Is there a Support Lifecycle Policy within the organization for the software in question? timeline?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
129.	A	Packs be distributed to the Acquirer?		
130.	B	What services does the help desk, support center, or (if applicable) online support system offer?		
131.	A/B	How extensively are patches and Service Packs tested before they are		
132.	A	Can patches and Service Packs be uninstalled? Are the procedures for uninstalling a patch or Service Pack	Yes☐ No☐ NA ☐	
133.	A/B	How are reports of defects, vulnerabilities, and security incidents involving the software collected,		
134.	A	How do you set the relative severity of defects and how do you prioritize their remediation?		
135.	A	What are your policies and practices for reviewing design and architecture security impacts in		
136.	A	Are third-party developers contractually required to follow your configuration management	Yes☐ No☐ NA ☐	
137.	B	What policies and processes does your company use to verify that software components do not contain unintended, “dead,” or malicious code? What tools are		
138.	B	How is the software provenance verified (e.g. any checksums or		
139.	A	Does your company publish a security section on its Web site? If so, do security researchers have the ability	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
140.	A	Does your company have an executive-level officer responsible for the security of your company’s software products and/or processes?	Yes☐ No☐ NA ☐	
141.	A	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.	Yes☐ No☐ NA ☐	
142.	A	Are security requirements developed independently of the rest of the requirements engineering activities, or are they integrated into the		
143.	A/B/D	What security design and security architecture documents are prepared as part of the SDLC process? How are they maintained? Are they available		

144.	B	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	Yes☐ No☐ NA ☐	
145.	B	Does the software use closed-source Application Programming Interfaces (APIs) that have undocumented	Yes☐ No☐ NA ☐	
146.	A	Does the organization 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	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
147.	B	How does the software's exception handling mechanism prevent faults from leaving the software, its resources, and its data (in memory		
148.	B	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	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
149.	B	Does the documentation explain how to install, configure, and/or use the software securely? Does it identify options that should not normally be used because they create security	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
150.	A	Does the software have any security critical dependencies or need additional controls from other software (e.g., operating system, directory service, application), firmware, or	Yes☐ No☐ NA ☐	
151.	A	What risk management measures are used during the software's design to mitigate risks posed by use of third-		
152.	A	Does your company's defect classification scheme include	Yes☐ No☐ NA ☐	
153.	B	What percentage of code coverage does your testing provide?		
154.	B	When does security testing occur during the SDLC (e.g., unit level, subsystem, system, certification and		
155.	A	Is a validation test suite or diagnostic available to validate that the application software is operating correctly and in a secure configuration	Yes☐ No☐ NA ☐	
156.	B	Does your company develop security measurement objectives for phases of the SDLC? Has your company identified specific statistical and/or qualitative analytical techniques for measuring attainment of security	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	

157.	B	How is the assurance of software produced by third-party developers		

158.	D	How are trouble tickets submitted? How are support issues, specifically those that are security related,		
159.	A	Are help desk or support center personnel internal company resources or are these services		
160.	A	Are any of the services you plan to use located offshore, examples include data hosting, data processing, help desk and transcription services?	Yes☐ No☐ NA ☐	
161.	B	Does your company have a vulnerability management and reporting policy? Is it available for	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
162.	A	Does your company perform background checks on members of the software development team? If so, are there any additional “vetting” checks done on people who work on critical application components, such as security? Explain.	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
163.	B	Does your company have formally defined security policies associated with clearly defined roles and responsibilities for personnel working within the software	Yes☐ No☐ NA ☐	
164.	A	Has civil legal action ever been filed against your company for delivering or failing to correct defective software? Explain.	Yes☐ No☐ NA ☐	
165.	A	Please summarize your company’s history of ownership, acquisitions, and mergers (both those performed by your company and those to which		
166.	A	Is the controlling share (51+%) of your company owned by one or more non-U.S. entities?	Yes☐ No☐ NA ☐	
167.	A	What are your customer confidentiality policies? How are		
168.	D	What are the policies and procedures used to protect sensitive information from unauthorized access? How are the policies enforced?		
169.	A	What are the set of controls to ensure separation of data and security information between different customers that are physically located in the same data center? On the same		
170.	A	Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all	Yes☐ No☐ NA ☐	
171.	A	What are your policies and procedures for hardening servers?		
172.	A	What are your data backup policies and procedures? How frequently are your backup procedures verified?		

173.	A	What are the procedures for evaluating any vendor security alerts and installing patches		
		and Service Packs?		
174.	A	Is testing done after changes are made to servers? What are your rollback procedures in the event of problems resulting from installing a patch or Service Pack?	Yes☐ No☐ NA ☐	
175.	A	If you have agents or scripts executing on servers of hosted applications and what are the procedures for reviewing the security		
176.	A	What are the procedures and policies used to control access to the servers? Are audit logs maintained?		
177.	A	What are your procedures and policies for handling and destroying sensitive data on electronic and		
178.	A	Do you have a formal disaster recovery plan? What actions will be taken to recover from a disaster? Are warm or hot backups available?	Yes☐ No☐ NA ☐	
179.	A	Is two-factor authentication used for administrative control of all security devices and critical information	Yes☐ No☐ NA ☐	
180.	A/D	How are virus prevention, detection, correction, and updates handled for the		
181.	D	What type of firewalls (or application gateways) do you use? How are they		
182.	D	What type of Intrusion Detection System/Intrusion Protection Systems (IDS/IPS) do you use? How are they		
183.	A/D	Explain or provide a diagram of the architecture for the application including security mitigation.		
184.	A	Do you perform regular reviews of system and network logs for security	Yes☐ No☐ NA ☐	
185.	A	Do you have an automated security event management	Yes☐ No☐ NA ☐	
186.	A	What are your procedures for intrusion detection, incident response, and incident		
187.	A	Will you provide on-site support 24x7 to resolve security	Yes☐ No☐ NA ☐	
188.	A	Are security logs and audit trails protected from tampering or	Yes☐ No☐ NA ☐	
189.	A	How do you control physical and electronic access to the log files? Are log files consolidated to single		

190.	A	Do you provide security performance measures to the customer at regular intervals?	Yes☐ No☐ NA ☐	
191.	A	Describe your security testing processes.		
192.	A	Do you perform penetration testing of the service? If yes, how frequently are penetration tests performed? Are the tests performed by internal resources	Yes☐ No☐ NA ☐	
193.	A	The state does not allow applications to be placed on the state's system, or the state's system to connect to another system, or the consultant to store or process state data without first doing security scans. The state would want to scan a test system not a production system, are either of these an issue, if	Yes☐ No☐ NA ☐	
194.		It is state policy that if your system connects to another system providing SaaS, IaaS, or PaaS that this system has a security scan. The state would want to scan a test system not a production system, is this an issue, if so	Yes☐ No☐ NA ☐	
195.	A	How frequently is the security tests performed? Are the tests performed by internal resources		
196.	A	Do you have a SOC 2 audit report? Is the audit done annually? Does the audit cover all 5 of the trust principles? Does the audit include subservice providers? Has the auditor always been able to attest to an acceptable audit result? Will you provide a copy of your latest SOC 2 audit upon request, a	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
197.		Are you ISO 270001 certified? Is the certification done annually? Will you provide a copy of your certification	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
198.		(Use if PHI is involved) Are you HITRUST certified? Is the certification done annually? Will you provide a	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
199.		(Use if PHI is involved) Will this application now or possibly in the future share PHI with other	Yes☐ No☐ NA ☐	
200.	A	Are you or if the data is being hosted by a subservice provider are they FedRAMP certified?	Yes☐ No☐ NA ☐	
201.	B	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)?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	

202.	A/B	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		
203.	A/B	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? If yes summarize the contractual requirements. If yes how do you evaluate the third-party's adherence	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
204.	A/D	Do you have a BYOD policy that allows your staff to put any sort of protected state data on their device personal device(s) or other non- company owned system(s)?	Yes☐ No☐ NA ☐	
205.		What is your process for ensuring default remote login protocols and default passwords are disabled on the IoT devices that are connected to your system either permanently or intermittently?		
206.		What is your process for insuring the software on your IoT devices that are connected to your system, either permanently or intermittently, is maintained and updated?		
207.		(For PHI only) Have you done a risk assessment, if yes will you share it? If you have not done a risk assessment would you be willing to do one based on the Health and Human Services assessment tool (https://www.healthit.gov/providers-professionals/security-risk-assessment-tool) if yes will you share it? The state is willing to sign a Non-disclosure Agreement before viewing any risk assessment. If you have not done a	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	

208.		Do you require multifactor authentication be used by employees and subcontractors who have potential access to legally protected state data? If yes please explain your practices on multifactor authentication include the authentication level used as defined in NIST 800-63 in your explanation. If no do you plan on going to multifunction authentication, if so when?	Yes☐ No☐ NA ☐	