STATE OF SOUTH DAKOTA OFFICE OF

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

24/7 Sobriety Program Monitoring Software RFP

PROPOSALS ARE DUE NO LATER THAN January 20th, 2017

RFP #: 818

BUYER: South Dakota Attorney General's Office (SD ATG)
EMAIL: RFP818ATG247@state.sd.us

READ CAREFULLY

FIRM NAME:	AUTHORIZED SIGNATURE:
ADDRESS:	TYPE OR PRINT NAME:
CITY/STATE:	TELEPHONE NO:
ZIP (9 DIGITS):	FAX NO:
FEDERAL TAX ID#:	E-MAIL:

PRIMARY CONTACT INFORMATION

CONTACT NAME:	TELEPHONE NO:
FAX NO:	E-MAIL:

---

1 GENERAL INFORMATION

1.1 STANDARD CONTRACT TERMS AND CONDITIONS

Any contract or agreement resulting from this RFP will include the SD ATG's standard contract terms listed in Appendix B, along with any additional contract terms as negotiated by the parties. As part of the negotiation process the contract terms listed in 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 indicate that there are any issues with any contract terms then SD ATG will assume those terms are acceptable to the Offeror.

1.2 BIT STANDARD CONTRACT TERMS AND CONDITIONS

Any contract or agreement resulting from this RFP will include the State's standard I/T contract terms listed in Appendix C for a Vendor Hosted Proposal or Appendix D for a State Hosted Proposal along with any additional contract terms as negotiated by the parties. As part of the negotiation process the contract terms listed in Appendix C for a Vendor Hosted Proposal or Appendix D for a State Hosted Proposal 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 indicate that there are any issues with any contract terms then the State will assume those terms are acceptable to the Offeror. There is also a list of technical questions, Security and Vendor Questions which is attached as Appendix E. These questions must be answered and may be used in the proposal evaluation.

1.3 COOPERATIVE PURCHASING

The State of South Dakota, acting through its Bureau of Administration, Office of Procurement Management is soliciting proposals to establish a cooperative purchasing contract that will be made available to North Dakota and other states, under SDCL 5-18A-37

1.3 PURPOSE OF REQUEST FOR PROPOSAL (RFP)

1.3.1 Background: The South Dakota Attorney General's Office (SD ATG) currently has a 24/7 sobriety program monitoring and data collection software throughout the State. This program is run by local Sheriff's offices and administered by South Dakota Program Coordinator and Staffed by the SD ATG. This program includes twice a day PBT testing, UA testing, Drug patches, SCRAM Bracelets, and Ignition Interlock Devices. This program currently utilizes a 24/7 online application to record and maintain participant and testing information.

1.3.2 Goals and Objectives: The SD ATG currently has a 24/7 sobriety program monitoring and data collection software in place. SD ATG would like to replace the 24/7 sobriety program monitoring and data collection software that can includes the current software's capabilities as well as to increase stability of the program, improve the availability of data collection for reports, add additional features and give the program room to grow.

1.3.3 Description of Components or Phases: Open to replacement options. Option 1: State Hosted Solution. Option 2: Vendor Hosted Solution.

1.3.4 Scope of components or Phases: The four phases are expected to have the following components:

- **1.3.4.1** Phase one will include the following
  - **1.3.4.1.1** Successful product demonstration (At the discretion of SD ATG the demonstration can include onsite testing, integrity testing and conversion features)
  - **1.3.4.1.2** Negotiate and sign the contract
  - **1.3.4.1.3** Kick off meeting, which is expected to be onsite and include all project staff, technical support, and end user representation
  - **1.3.4.1.4** Establish initial project timeline and project plan
  - **1.3.4.1.5** Establish team assignments
  - **1.3.4.1.6** Finalize solution requirements
  - **1.3.4.1.7** Establish testing and exercise requirements including identifying external testing agencies
  - **1.3.4.1.8** Establish the time the system needs to operate trouble free for final acceptance
- **1.3.4.2** Phase two will include the following:
  - **1.3.4.2.1** Customize the product as needed

1.3.4.2.2 Set up the test system
1.3.4.2.3 Integration testing
1.3.4.2.4 Functional testing
1.3.4.2.5 Performance testing
1.3.4.2.6 Load testing
1.3.4.2.7 Data Conversion
1.3.4.2.8 Completion of security requirements (As agreed in the final contract)
1.3.4.3 Phase three testing will include the following:
1.3.4.3.1 UAT testing
1.3.4.3.2 Training onsite
1.3.4.4 Phase four will include the following:
1.3.4.4.1 Push the system out Statewide
1.3.4.4.2 Resolution of any problems found
1.3.4.4.3 Additional training as needed
1.3.4.4.4 Allow system to operate trouble free for a predetermined period of time

The proposal may include a project plan with different phases but any project plan must include as a minimum the items list above. Deviation from the phases listed about should be explained as stated in 7.5. Completion of the final item in each phase will be the milestone for that phase. Payment will be based on the successful completion of each milestone. The percentage paid for each completed phase is negotiable.

1.4 ISSUING OFFICE AND RFP REFERENCE NUMBER

The SD ATG is the issuing office for this document and all subsequent addenda relating to it, on behalf of the State of South Dakota, ATG. The reference number for the transaction is RFP# 818. This number must be referred to on all proposals, correspondence, and documentation relating to the RFP.

1.5 LETTER OF INTENT

It is preferred that all interested Offerors submit a **Letter of Intent** to respond to this RFP.

The letter of intent must be received by the SD ATG no later than Dec.16th, 2016. If submitted by mail the envelope should be addressed to:

SD Attorney General's Office
Attn: 24/7 RFP #818
1302 E Hwy 14, Suite 5,
Pierre, SD 57501-8505

Be sure to reference the RFP number in your letter.

The Letter of Intent may be submitted to the email address RFP818ATG247@state.sd.us.

1.6 SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)

RFP Publication: December 1st, 2016
Letter of Intent to Respond Due: December 16th, 2016
Deadline for Completion of Site Visits: January 6th, 2017
Deadline for Submission of Written Inquiries: January 6th, 2017
Responses to Offeror Questions: January 13th, 2017
Proposal Submission Deadline: January 20th, 2017
Evaluation of Proposals to Determine Short List: January 27th, 2017
Demonstrations and presentations: February 6th – 10th 2017 and February 13th – February 17th, 2017
Discussions: Week of February 20th, 2017
Anticipated Award Decision/Contract Negotiation: February 27th, 2017

1.7 SUBMITTING YOUR PROPOSAL

All proposals must be completed and received in the SD ATG 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 5 identical copies of the proposal shall be submitted. Offerors must also provide a secure location where SD ATG can electronically obtain the Offeror's proposal(s)**.**

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 intended by the respondent. 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 #818 PROPOSAL TITLE 24/7 Sobriety Program Monitoring Software RFP

DUE: January 20th, 2017
BUYER: South Dakota Attorney General's Office
Attention: 24/7 RFP # 818
Address: 1302 E Hwy 14, Suite 5
Pierre, SD 57501-8505

No proposal shall be accepted from, or no contract or purchase order shall 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.

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

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

1.9 NON-DISCRIMINATION STATEMENT

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

1.10 MODIFICATION OR WITHDRAWAL OF PROPOSALS

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

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

1.11 OFFEROR INQUIRIES

All written questions should be sent to: RFP818ATG247@state.sd.us, only emailed questions will be accepted.

Offeror may submit email questions concerning this RFP to obtain clarification of requirements. No questions will be accepted after the date and time indicated in the above schedule of activities. Email questions to the email address listed above with the subject line "RFP# 818". The questions and their answers will be posted on the SD ATG Website at http://atg.sd.gov/OurOffice/rfp.aspx before the proposal submittal date and will be posted by the date and time indicated in the above calendar of events. Offeror may not rely on any other statements, either of a written or oral nature, that alter any specification or other term or condition of this RFP that have not originated from the SD RFP Project Contact. Offerors will be notified in the same manner as indicated above regarding any modifications to this RFP.

1.12 PROPRIETARY INFORMATION

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

1.13 LENGTH OF CONTRACT

The contract will begin on April 1st, 2017.
The contract will end on October 1st, 2017
If first year maintenance is included in proposal, contract end date will be negotiable.

1.14 SITE VISIT

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

1.15 PRESENTATIONS/DEMONSTRATIONS

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

1.15 DISCUSSIONS

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

1.16 NEGOTIATIONS

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

2.0 SCOPE OF WORK

The new 24/7 software must be able to retain all of its current functions as well as be able to perform the requirements outlined in Appendix A.

3.0 RESOURCES

The Bureau of Information and Telecommunications (BIT) is the State organization that provides IT services for the State.

Historically, the most successful projects are those that use the team approach. The team approach utilizes a combination of Offeror staff, BIT staff, and Agency staff. Below is a description of how the team will be structured.

3.1. TEAM ORGANIZATION: Provide the following information.

3.1.1 PROJECT ORGANIZATION CHART

List names, job titles (designate vacancies), and the city and state in which individual will work on this project.

3.1.2 LIST OF ALL VENDORS AND SUBCONTRACTORS

List all entities to be used for performance of the services described in this RFP. In the work plan, describe which responsibilities will be assigned to vendors or subcontractors and the city and state in which the vendors or subcontractors are located.

3.2 PROJECT STAFFING ROLES

Agency Project Sponsor

Agency Director

Role: Some of the duties performed by the Agency Project Sponsor are:

- Resolves resource and priority conflicts
- Approves the Project Charter and/or Plan
- Holds subordinate managers accountable for their performance
- Has a direct communications and reporting relationship with the Agency Project Manager
- Is the chief advocate for the project
- Keeps the team focused on appropriate goals
- Keeps the team updated with new information
- Holds the project team accountable for planning and executing the project
- Holds the team accountable for delivering agreed-upon results

Agency Project Manager

24/7 Program Coordinator

Role: Some of the duties performed by the Agency Project Manager are:

- Day to day oversight of the project
- Approves vendor payments based on contract/work order language
- Provides direction to Agency employees as well as the team

Reports to: The Agency Project Sponsor. This person must keep the Project Sponsor informed on a weekly basis regarding progress and status of the project. When issues arise, this person must be able to make recommendations to the team regarding amendments and changes to the deliverables, schedule or budget.

Agency IT Team Leader

Agency IT Team Leader

Role: Some of the duties of the Agency IT Team Leader are:

Supervises Agency IT Project Manager
In close daily contact with Agency Project manager and Agency IT Project Manager to ensure that all requirements are fulfilled.
Able to advise the Agency Project Manager of cost/benefit as well as consequences of any changes in work direction

Reports to: Agency Project Sponsor

Agency IT Project Manager

Agency Computer Support Specialist

Role: Some of the duties performed by the Agency IT Project Manager are:

- Main contact with vendor regarding project status and progress
- In close daily contact with the Agency Project Manager and Agency IT Team Leader to ensure that all requirements are fulfilled
- Able to advise the Agency Project Manager of cost/benefit as well as consequences of any changes in work direction

Reports to: Agency IT Team Leader

Project Steering Team

Statistical Analysis Staff
ATG Attorney Staff
BIT Agency POC

Role: Some of the duties performed by the Project Steering Team:

- Oversee the project in terms of the contract and work order agreements. Specific items of oversight include:
  - What are the deliverables for his or her agency, and are they being met?
  - Is the project on schedule? If not, what are the consequences? Should the project be put back on schedule and how will that be done?
  - What expenditures have been made? Is the project on budget? If not, what are the circumstances surrounding it?
- Recommendation of approval of any scope changes, or any changes that affect cost and schedule based on cost benefit to the Project Owner

Reports to: Their Agency Manager.

Authority: Each Steering Team member should have authority to make decisions for their own departmental area.

3.3 STAFF RESUMES AND REFERENCES

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

- Name
- Title
- Contact Information (telephone number(s), e-mail address)
- Work Address
- Project Responsibilities (as they pertain to this project)
- Percentage of time designated to this project
- Brief listing of Work Experience in reverse chronological order from present to January, 2012 (only provide company name, job title(s)/position(s) held, date started and date left each position, brief description of job duties, responsibilities, and significant accomplishments)
- RFP Project Experience
- Technical Background relative to this project

- Experience in Similar Projects
- Names of the Similar Projects they were involved in
- Role they played in the projects similar to this project
- Project Management Experience
- Technical Knowledge
- Education
- Relevant Certifications
- Three Professional References (name, telephone number, company name, relationship to employee)

4.0 PROJECT DELIVERABLES/APPROACH/METHODOLOGY

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

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

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

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

All software and cloud services purchased by SD ATG will be subjected to security scans by BIT without exception.

Security scanning will be performed during the software development phase and during pre-production review. These scans and tests can be time consuming and should be allowed for in project planning documents and schedules. Products that do not meet BIT's security and performance requirements will not be allowed to go into production and may be barred from UAT until all issues are addressed to SD ATG's satisfaction. SD ATG urges the use of industry scanning/testing tools and secure development methods be employed to avoid unexpected costs and project delays. Costs to produce and deliver secure and reliable applications are the responsibility of the software entity producing or delivering an application to SD ATG. Unless expressly indicated in writing, SD ATG assumes all price estimates and bids are for the delivery and support of applications and systems that will pass security and performance testing.

As part of this project the Offeror will provide a monitoring tool SD ATG can utilize to monitor the operation of the proposed solution as well as all systems and all subcomponents and connections. It is required that this tool be easy to use and provide a dashboard of the health of the proposed solution. The effectiveness of this monitoring tool will be a component of the acceptance testing for this project.
As part of the project plan the Offeror will include development of an implementation plan that includes a back out component. Approval of the implementation plan by BIT should be a project milestone. Should the implementation encounter problems that cannot be resolved and the implementation cannot proceed to a successful conclusion the back out plan will be implemented. The Implementation and back out documentation will be included in the project documentation.

The successful Offeror will use the approved BIT processes and procedures when planning their project in particular the change management process. Work with the respective agency's BIT Point of Contact on this form. The Change Management form is viewable only to BIT employees. The purpose of this form is to alert key stake holders (such as: Operations, Systems Support staff, Desktop Support staff, administrators, Help Desk personnel, client representatives,

and others) of changes that will be occurring within state resources and systems to schedule the:

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

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

Include in your submission details on your:

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

4.1 Testing: Will include external testing by law enforcement agencies

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

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

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

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

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

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

If the software is being hosted on the State systems regression testing and integration testing is done by the vendor with assistance of BIT Development. If the software is being hosted on the State systems functional testing is generally done by the vendor and the agency with assistance of BIT Development. If the software is being hosted on the State systems performance testing and load testing is generally done by BIT Telecommunications division. If the vendor is hosting the software on their systems regression testing, if relevant, integration testing, if relevant, functional testing, performance and

load testing should be done by the vendor. The UAT is generally done by the vendor and the agency, whether the software is hosted on the State's or the vendor's systems. All testing is done in test environments either set up by the vendor or by BIT. All test results should meet the requirements of the agency before the software goes into production. For a software development project; at a minimum regression, integration, functional, and UAT must be done when software is being customized; if software is being developed fresh at a minimum integration, functional, and UAT tests must be done. Assuming no problems are found you should plan on a minimum of three weeks for performance and load testing if done by BIT.

SD ATG, at its sole discretion, may consider a solution that does include all or any of these deliverables or consider deliverables not originally listed. An Offeror **must** highlight any deliverable they do not meet and give any suggested "work-around" or future date that they **will** be able to provide the deliverable.

5.0 FORMAT OF SUBMISSION

All proposals should be prepared simply and economically and provide a direct, concise explanation of the Offeror's proposal and qualifications. Elaborate brochures, sales literature and other presentations unnecessary to a complete and effective proposal are not desired.

Offerors are required to provide an electronic copy of their response. The electronic copy should be provided in MS WORD or in PDF format, except for the project plan, which must be in MS Project or MS Excel . The submission must be delivered as indicated in Section 1.7 of this document.

The Offeror is cautioned that it is the Offeror's sole responsibility to submit information related to the evaluation categories and that the State of South Dakota is under no obligation to solicit such information if it is not included with the proposal. The Offeror's failure to submit such information may cause an adverse impact on the evaluation of the proposal. You should respond to each point in the Scope of Work and Deliverables in the order they were presented.

Offerors and their agents (including subcontractors, employees, vendors, or anyone else acting on their behalf) must direct all of their questions or comments regarding the RFP, the evaluation, etc. to SD ATG, Attn: 24/7 RFP # 818. Offerors and their agents may not contact any state employee other than the SD ATG office at RFP818ATG247@state.sd.us regarding any of these matters during the solicitation and evaluation process. Inappropriate contacts are grounds for suspension and/or exclusion from specific procurements. Offerors and their agents who have questions regarding this matter should contact the SD ATG office atRFP818ATG247@state.sd.us.

The Offeror may be required to submit a copy of their most recent audited financial statements upon SD ATG's request.

The proposal should be page numbered and should have an index and/or a table of contents referencing the appropriate page number. Each of the sections listed below should be tabbed.

Offerors are cautioned that use of the State Seal in any of their documents is illegal as per South Dakota Codified Law 1-6-3.1. *Use of seal or facsimile without authorization prohibited--Violation as misdemeanor. No person may reproduce, duplicate, or otherwise use the official seal of the State of South Dakota, or its facsimile, adopted and described in §§ 1-6-1 and 1-6-2 for any for-profit, commercial purpose without specific authorization from the secretary of state. A violation of this section is a Class 1 misdemeanor.*

Proposals should be prepared using the following headings and in the order that they are presented below. Please reference the section for details on what should be included in your proposal.

5.1 Statement of Understanding of Project
5.2 Corporate Qualifications
5.3 Relevant Project Experience
5.4 Project Plan
5.5 Deliverables
5.6 Non Standard Software and Hardware

5.1 STATEMENT OF UNDERSTANDING OF PROJECT

To demonstrate your comprehension of the project, please summarize your understanding of what the work is and what the work will entail. This should include, but not be limited to your understanding of the purpose and scope of the project,

critical success factors and potential problems related to the project and your understanding of the deliverables. Your specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements should be included. This section should be limited to no more than two pages.

5.2 CORPORATE QUALIFICATIONS

Please provide responses to the each of the following questions in your proposal.

A. What year was your parent company (if applicable) established?

B. What is the business of your parent company?

C. What is the total number of employees in the parent company?

D. What are the total revenues of your parent company?

E. How many employees of your parent company have the skill set to support this effort?

F. How many of those employees are accessible to your organization for active support?

G. What year was your firm established?

H. Has your firm ever done business under a different name and if so what was the name?

I. How many employees does your firm have?

J. How many employees in your firm are involved in this type of project?

K. How many of those employees are involved in on-site project work?

L. What percent of your parent company's revenue (if applicable), is produced by your firm?

M. Corporate resources available to perform the work, including any specialized services, within the specified time limits for the project

N. Availability to the project locale

O. Familiarity with the project locale

P. Has your firm ever done business with other governmental agencies? If so, please provide references.

Q. Has your firm ever done business with the State of South Dakota? If so, please provide references.

R. Has your firm ever done projects that are like or similar to this project? If so, how many clients are using your solution? Please provide a list of four or more locations of the same approximant nature as SD ATG where your application is in use along with contact names and numbers for those sites. The State of South Dakota has a consolidated IT system. **Either** any references given should be from States with a consolidated IT system, to be acceptable **or** the reference should be a detailed explanation on how you will modify your work plan for a consolidated environment that you are unfamiliar with.

S. Provide third party security audits of the four projects you provided for R above. SD ATG will sign a non-disclosure statement, as needed, to receive these audits, within the limits of SD ATG's open records law. If there are no audits of these projects then provide, unedited and un-redacted results of such security testing/scanning from third-party companies and/or tools that has been run within the past 90 days. To protect proprietary or confidential information, SD ATG will agree to non-disclosure of any information provided as a result of such a request as appropriate.

T. What is your Company's web site?

When providing references, the reference must include the following information:

- 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
- Dates of the service/contract
- A brief, written description of the specific prior services performed and requirements thereof

5.3 RELEVANT PROJECT EXPERIENCE

Provide details about four recent projects that the Offeror was awarded and then managed through to completion. Project examples should include sufficient detail so the agency fully understands the goal of the project; the dates (from start to finish) of the project; the Offeror's scope of work for the project; the responsibilities of the Offeror and Subcontractors in the project; the complexity of the Offeror's involvement in the project; deliverables provided by the Offeror; the methodologies employed by the Offeror; level and type of project management responsibilities of the Offeror; changes that were made and request for changes that differed from the onset of the project; how changes to the project goals, Offeror's scope of work, and/or deliverables were addressed or completed; price and cost data; quality of the work and the total of what the Offeror accomplished in the project.

A. Client/Company Name

B. Client Company Address, including City, State and Zip Code

C. Client/Company Contacts(s)
   Name
   Title
   Telephone Number
   E-mail address
   Fax Number

D. Project Start Date

E. Project Completion Date

F. Project Description and Goals

G. Offeror's Role in Project

H. Offeror's responsibilities

I. Offeror's Accomplishments

J. Description of How Project Was Managed

K. Description of Price and Cost Data from Project

L. Description of special project constraints, if applicable

M. <u>Description of your ability and proven history in handling special project constraints</u>

N. Description of All Changes to the Original Plan or Contract That Were Requested

O. Description of All Changes to the Original Plan or Contract That Offeror Completed

P. Description of How Change Requests Were Addressed or Completed by Offeror

Q. Was Project Completed in a Timeframe That Was According to the Original Plan or Contact? (If "No", provide explanation)

R. Was Project Completed Within Original Proposed Budget? (If "No" provide explanation)

S. Was there any Litigation or Adverse Contract Action regarding Contract Performance? (If "Yes" provide explanation)

T. Feedback on Offeror's Work by Company/Client

U. Offeror's Statement of Permission for the Department to Contact the Client/Company and for the Client's/Company's Contract(s) to Release Information to the Department

5.4 PROJECT PLAN

Provide a project plan that indicates how you will complete the required deliverables and services and addresses the following:

- Proposed project management techniques
- Number of Offeror's staff needed
- Tasks to be performed (within phase as applicable)
- Number of hours each task will require
- Deliverables created by each task
- Dates by which each task will be completed (dates should be indicated in terms of elapsed time from project inception)
- Resources assigned to each task
- Required state agency support
- Show task dependencies
- Training (if applicable)

Microsoft Project is the standard scheduling tool for the State of South Dakota. The schedule should be a separate document, provided in Microsoft Project or Excel, and submitted as an attachment to your proposal.

If as part of this project, the Offeror plans to set-up or configure the software and/or hardware and plans to do this outside of South Dakota, even in part, then they need to provide a complete and detailed project plan on how the Offeror plans on migrating to SD ATG's site. Failure to do this is sufficient grounds to disregard the submission, as it demonstrates that the Offeror fundamentally does not understand the project. Providing a work plan for the steps above that is complete and detailed maybe sufficient.

5.5 DELIVERABLES

This section should constitute the major portion of the work to be performed. Provide a complete narrative detailing the assessment of the work to be performed, approach and methods to provide the requirements of this RFP, the Offeror's ability to fulfill the requirements of this RFP, the Offeror's approach, the resources necessary to fulfill the requirements, project management techniques, specialized services, availability to the project locale, familiarity with the project locale and a description of any options or alternatives proposed. This should demonstrate that the Offeror understands the desired overall performance expectations. This response should identify each requirement being addressed as enumerated in section 8.0. If you have an alternative methodology or deliverables you would like to propose, please include a detailed description of the alternative methodology or deliverables and how they will meet or exceed the essential requirements of the methodology and deliverables described in Section 6.0.

5.5.1 The Vendor shall develop design documents to include the technical architecture and system design of the application. This documentation shall contain the architectural diagrams as well as system configuration and any custom development to the application. The documentation shall be detailed enough for reviewers to understand the function and appearance of all screens.

5.5.2 Interfaces — The Vendor shall be responsible for implementing all aspects of the interfaces described in the Technical Requirements. The Vendor shall be responsible for working with the Agency Project Manager and Agency IT Project Manager to understand the technical interface requirements.

5.5.3 Hardware — If a state hosted solution is proposed, upon award, the Vendor shall work with the SD ATG and SD BIT to understand the existing infrastructure, assess hardware and software compatibility, and gather information on licenses available for use on this project. The findings of these examinations shall be compiled by the Vendor and submitted to the Agency Project Manager. All Vendor warranty and licensing agreements associated with this system shall be in the name of the SD ATG. The Vendor shall install, test and commission all software required to support the system.

LLEAs shall be responsible for providing user workstations. SD ATG/BIT shall discuss any suggested network enhancements. The Vendor's responsibilities are limited to suggesting the improvements to network infrastructure during proposal submission and as a result of the design efforts.

5.5.4 Acquisistion of third party applications or data bases for RFPSThe acquisition of any third-party software, hardware or databases needed to fulfil the project's contract requires the active participation of the State. The State must approve the costs as well as the terms and conditions of the acquisition of each individual item. The terms and conditions of the acquisition of any open source or freeware software must be also be approved by the State before

acquisition. Project plans should allow sufficient time for the acquisition process.

5.5.5 Application Software Code — Preference will be given to Vendor solutions which deliver all application software code to SD ATG in an acceptable format (DVD, tape, ftp site, etc.).

5.5.6 Technical Documentation — If proposing State hosted solution, System and Technical Documentation sufficient for SD ATG IT to maintain and support the system shall be provided by the selected Vendor, including documentation for the software application, data repository, data interfaces, network etc.

5.5.7 Detailed Project Schedule and milestones with delivery dates showing sub-projects activities and tasks, milestones and targeted delivery data and resources required and allocated to each. The Project Schedule shall be updated on a weekly basis in MS Project and submitted to the Agency Project Manager and Agency IT Project Manager.

5.5.8 Plan of Work — a subordinate document made following establishment of a contract with the awarded Vendor and acceptance of a Project Management Plan. One or more SOWs may be used to provide specific details regarding migration, testing, acceptance and related project work, but may not modify the terms of the contract.

5.5.9 Weekly Status/ Progress Reports that reflect the current status of each active project task, projection of work to be performed the next week, alerts of potential problems and schedule delays and risk mitigation plans.

5.5.20 The Vendor's organization chart and staffing table with names and title of personnel assigned to the project. This shall be in agreement with staffing of accepted proposal. Necessary substitutions due to change of employment status and other unforeseen circumstances may only be made with prior approval of SD ATG. Resumes shall be included with the organizational chart for all Vendor staff assigned to the project.

5.5.11 Each project milestone shall have individual Acceptance Criteria which detail the completion of the specific milestone. The Acceptance Criteria are to be mutually developed by the Agency and the awarded Vendor and reduced to writing within forty-five (45) days after the contract award. Vendor payments shall be made pursuant to the Payment Plan that corresponds to each completed milestone as negotiated between the parties.

5.5.12 Communications Plan including contact list, meetings, document distributions, reports, etc.

5.5.13 Issue & Risk Management Plans and Logs—documented plans for logging and managing issues and risks, as well as the associated tracking logs jointly maintained by the Vendor and SD ATG Project Manager, to be reviewed / updated weekly.

5.5.14 Action Item Log — tracking all open project related action items, assignments and due dates jointly maintained by the Vendor and SD ATG Project Manager, to be reviewed / updated weekly.

5.5.15 Staffing and Resource Management Plan — indicates people, system, and network resources required for this procurement by month. This plan shall cover both Vendor and SD ATG/BIT resources.

5.5.16 Configuration Management Plan — describing the version control methodology that shall be in place to manage documentation versions and software releases.

5.5.17 Change Management Plan and a change control board (CCB) comprised of the Vendor, the Development Team Project Manager, the Agency Project Sponsor or Assistant, the Agency IT Project Manager and the Agency Project Manager, are jointly to decide on any changes to this project, pursuant to a mutually agreeable change process that shall be set out as part of the project plan. The CCB shall meet on an ad hoc basis when changes are necessary to the project and, if also needed, to the contract. The RFP terms and conditions shall be followed when implementing any changes to the contract, including any necessary State Procurement approvals.

5.5.18 Test Plans - including Integration Testing, User Acceptance Testing, Load Testing and documented test results. Vendor shall recommend specific test levels and structured test environment required for this contract for SD ATG's approval.

5.5.19 Acceptance Plan shall define the process to be followed and criteria for acceptance of each milestone and deliverable. The Acceptance Plan shall include the following elements: Introduction (including the purpose of the Acceptance Plan, Scope, Definitions, References, and Overview), Roles and Responsibilities, Acceptance Tasks, Criteria

for Milestones and Deliverables (Section 6), Problem Resolution and Corrective Action, Acceptance Environment and Deliverable/Service Acceptance.

5.5.20 Payment Plan: payment to the awarded Vendor shall be upon the completion and acceptance by SD ATG of each milestone as defined in the project schedule pursuant to Section 6.0, and Payment Terms. The value of each milestone shall be established in the Vendor's Cost Proposal and negotiated and agreed upon during the contract negotiations phase. Any payment change request shall require submission to and approval of SD ATG. The Vendor shall provide an annual payment plan for the life of this contract if requested by SD ATG.

5.5.21 Quality Management Plan describes the Vendor's method of testing the system and ensuring defects are identified and resolved. Upon award of contract, the Vendor and SD ATG Project Manager shall create the quality management plan together as part of the project management plan development stage. The final version shall be accepted by the Agency in writing before Vendor may proceed with implementation of the Contract. The quality management methodology that shall be used in this Contract shall be included in the Quality Management Plan.

5.5.22 Implementation Plan — describes how the Vendor's solution shall be deployed, installed and transitioned into an operational system. The plan contains an overview of the system, a brief description of the major tasks involved in the implementation, the overall resources needed to support the implementation effort (such as hardware, software, facilities, materials, and personnel), and any site-specific implementation requirements. The implementation schedule shall be mutually agreed upon and set between SD ATG and the Vendor.

5.5.23 Disaster Recovery Plan — If proposing a Vendor hosted solution, Vendor shall provide a detailed plan describing the approach to disaster recovery for enabling the software to come back online; including failover/restore capabilities from single server hard drive failure to entire server failure, etc. A detailed test plan to test the various failover/recovery aspects shall be included. The final disaster recovery plan will need to be vetted and approved upon vendor selection and working in conjunction with SD ATG IT/BIT staff. If proposing a State hosted solution, meeting state hosted standards, this will provided by BIT. A disaster recovery plan for the 24/7 program should have a downtime of no more than 12 hours.

5.6 NON STANDARD SOFTWARE AND HARDWARE

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

If non-standard software and or hardware are used the project plan and the costs stated in 8.7 will have to include service desk and field support, since BIT can only guarantee best effort support for standard hardware and software. If any software development may be required in the future hourly development rates should also be stated. The project plan should also include the development and implementation of a disaster recovery plan since non-standard software and hardware will not be covered by the State's disaster recovery plan. This should also be reflected in the costs.

There is also a list of technical questions, Security and Vendor Questions which is attached as Appendix E. These questions must be answered, and signed by the Offeror and may be used in the proposal evaluation.

6.0 COST PROPOSAL

Offerors may submit multiple cost proposals. All costs related to the provision of the required services must be included in each cost proposal offered.

Cost will be evaluated as part of the technical proposal. Offerors may submit multiple costs in their proposal. All costs related to the provision of the required services must be included in each proposal offered.

The Offeror shall submit a statement in the Proposal that attests the Offeror's willingness and ability to perform the work described in this RFP for the price being offered. The Offeror shall submit a statement in the Cost Proposal that attests the Offeror's willingness and ability to perform the work described in this RFP for the price being offered.

6.1 STAFFING

Name	Role	Total Hours on Project	Total Hours on Site	Hourly Rate	Total
				Total:	

6.2 TRAVEL AND EXPENDITURE TABLE

Name	Method of Travel	Cost per trip	Number of Trips	Total Cost
			Total:	

Name	Lodging Cost per night	Number of Nights	Lodging Cost	Per diem	Number of Days	Per diem Cost	Total Cost
Totals:							

NOTE: SD ATG asks that vendors accept state per diem. Lodging per diem is $55/night and is readily achievable in South Dakota. Food per diem is $26/day.

6.3 OTHER COSTS

Show any other costs such as: software, hardware, ongoing costs, etc.

	One Time	Year 1	Year 2	Year 3	Totals
Hardware					
Software					
Maintenance					
License Fees					

Training					
Other…					
Totals					

6.4 ADDITIONAL WORK

The Offeror may be expected to perform additional work as required by any of SD ATG signatories to a contract. This work can be made a requirement by SD ATG for allowing the application to go into production. This additional work will not be considered a project change chargeable to SD ATG 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 should be included in your proposal.

7.0 PROPOSAL EVALUATION AND AWARD PROCESS

7.1

After determining that a proposal satisfies the mandatory requirements stated in the Request for Proposal, the evaluator(s) shall use subjective judgment in conducting a comparative assessment of the proposal by considering each of the following criteria:

7.2

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

7.3

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

7.4 Evaluation Criteria

7.4.1 Specialized expertise, capabilities and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements
Project Plan

7.4.1.1 Application software functionality

7.4.1.2 Training and documentation Options

7.4.1.3 Warranty and maintenance terms and tiers

7.4.1.4 Customer Service options

7.4.2 Proposed project management techniques

7.4.3 Resources available to perform the work, including any specialized services, with the specified time limits for the project.

7.4.3.1 Technical Environment

7.4.3.2 Timeline

7.4.4 Cost

7.4.4.1 Project cost

7.4.4.2 Maintenance cost

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

7.4.6 Ability and proven history in handling special project constraints

7.4.7 Availability to the project locale

7.4.8 Familiarity with the project locale

SD ATG reserves the right to reject any or all proposals, waive technicalities, and make award(s) as deemed to be in the best interest of SD ATG.

7.5 Award

The requesting agency and the highest ranked Offeror shall mutually discuss and refine the scope of services for the project and shall negotiate contract terms, including compensation and performance schedule.

7.5.1

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

7.5.2

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

8. BEST AND FINAL OFFERS

SD ATG reserves the right to request best and final offers. If so, SD ATG will initiate the request for best and final offers; best and final offers may not be initiated by an Offeror. Best and final offers may not be necessary if SD ATG is satisfied with proposals received.

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

South Dakota 24/7 Sobriety Program Webpage & Data Collection RFP Requirements and Requests (Art Mabry - November 2016)			
Ref #	**Description/Function**	**Revise**	**Name**
1.0	**Sign In**		
1.1	Username - First name initial, full last name		
1.2	Password - Set by User. Capable of being reset by Admin.		
1.3	New User Link - Used by a new User to set unique password		
1.4	List Admin contact for assistance including phone number and email link.		
1.5	OPTIONAL SIGNON CHANGE: single sign on authentication through RISS.NET using federated services.		
2.0	**Main Page (Rename: Home Page) - Site Administration**	X	
2.1	**No Show List -** Used to track Participants who haven't performed their scheduled testing		
2.1.1	Quick Link - No shows for AM and PM with link to alphabetized list		
2.1.2	Name (link to account), Test type, Balance, Link to apply No Show, Link to apply excused absence including reason.		
2.2	**Add Existing Participant** - Used when a Participant is enrolled at a testing site but needs to test at one or more other sites.		
2.2.1	Adding the Participant's account number adds the Participant to the new testing site.		
2.3	**State Account Disbursement (Rename: Agency State Participation Fee Payments)** - Participation Fees paid to AG for PBT.	X	
2.3.1	Add a Disbursement - Completed when payment made to AG (Amount, date and comments)		
2.3.2	From/To - Defaults to last 3 months. Capable of searching any duration or specific timeframe.		
2.3.3	List includes date, State fees owed that date by Participants, unpaid fees for that date, collected fees for the date, disbursements to AG and balance		
2.3.4	View Link - Goes to page that lists all the Participants owing State fee for that date, amount and paid/unpaid.		
2.3.5	Total State Fees -Total unpaid = Collected State Fees - Total Disbursements = Balance Change + Balance Forward = New Balance for period selected		
2.4	**SCRAM Payments to Disburse (Rename: SCRAM Payments Due to AG)** - SCRAM payments collected by testing site current balance.	X	
2.4.1	Add a Disbursement - Lists the amount of SCRAM fees owed to AG. Add Disbursement link sends it to Admin page and SCRAM Disbursement (History)		
2.4.2	Update - Changes the ending date of SCRAM payments received.		
2.4.3	List includes name link to Participants page, date payment received, amount and receipt number.		
2.5	**SCRAM Disbursements** - History of SCRAM payments.		
2.5.1	From/To - Defaults to last year. Capable of searching any duration or specific timeframe.		

2.5.2	Status - Received = Received by AG, Unreceived = Submitted but not received by AG and Undisbursed = Not paid yet.		
2.5.3	View Link - Goes to the details for the listed status.		
2.6	**Change Password** - Ability for individual User to change their password.		
2.7	**Manage User** - Ability for individual User to remove another agency User.		
	Reports		
2.8	**Account Activity** - Displays testing site activity for a specific date.		
2.8.1	Date - Can be manually changed.		
2.8.2	Shift - Selection of AM or PM		
2.8.3	Type - Payments, refunds, balance adjustments and test types		
2.8.4	Details - Used to customize the report.		
2.9	Participants - Detailed information regarding all the Participants who have been enrolled/tested at the testing site		
2.9.1	Agency - Search by the entity that placed the individual on the program.		
2.9.2	Court Reason - Search by the reason placed on the program **(Descriptions need clarification)**	X	
2.9.3	Judge - Search by a specific Judge		
2.9.4	Offense - Search by a specific offense		
2.9.5	Status - Search by Participant status		
2.9.6	Test Type - Search by specific test type.		
2.9.7	Fees - Search by waived fees		
2.9.8	Group By - Group by any of the above searches.		
2.9.9	Save to Spreadsheet Link - Save to Excel for searching and data formatting.		
2.10	**Repeat Participants** - Lists Participants who have been enrolled more than once.		
2.11	**SCRAM Days** - Lists SCRAM Participants total days on SCRAM during a specific timeframe.		
2.11.1	From/To - Defaults to the previous month. Capable of searching any duration or specific timeframe.		
2.11.2	List includes name link to Participants page, SCRAM site and total days.		
2.12	**SCRAM Participants** - Lists SCRAM details for each SCRAM Participant		
2.12.1	Lists SCRAM Site, name with link, date started/finished and financial information ref payments.		
2.13	**Summary** - Overview of activity including tests, financial and court reason		
2.13.1	From/To - Defaults to the last month. Capable of searching any duration or specific timeframe.		
2.13.2	Show - Switch between Days and Shifts		
2.13.3	Test Type - Search by specific test type.		
2.13.4	Agency - Search by the entity that placed the individual on the program.		
2.13.5	Court Reason - Search by the reason placed on the program (Descriptions need clarification)		
2.13.6	Date Link - Goes to Account Activity for the specific date.		
2.13.7	Save to Spreadsheet Link - Save to Excel for searching and data formatting.		
2.14	**Officer Test Counts** - Lists PBT and UA tests per testing officer		
2.14.1	From/To - Defaults to the previous month. Capable of searching any		

	duration or specific timeframe.		
2.14.2	Save to Spreadsheet Link - Save to Excel for searching and data formatting.		
2.15	**Unpaid Fees** - Lists unpaid fees for the testing site for Active and Inactive Participants (SCRAM fees are only activation/deactivation fees - not daily fees)		
2.15.1	Agency - Search by the entity that placed the individual on the program.		
2.15.2	Court Reason - Search by the reason placed on the program (Descriptions need clarification)		
2.15.3	Judge - Search by a specific Judge		
2.15.4	Offense - Search by a specific offense		
2.15.5	Test Type - Search by specific test type.		
2.15.6	Save to Spreadsheet Link - Save to Excel for searching and data formatting.		
2.16	**Unpaid SCRAM Fees** - Lists unpaid SCRAM daily fees for Active and Inactive Participants		
2.16.1	Agency - Search by the entity that placed the individual on the program.		
2.16.2	Court Reason - Search by the reason placed on the program (Descriptions need clarification)		
2.16.3	Judge - Search by a specific Judge		
2.16.4	Offense - Search by a specific offense		
2.16.5	Save to Spreadsheet Link - Save to Excel for searching and data formatting.		
2.17	**Temporary Removals** - Lists Participants with a Temporary Removal status		
2.17.1	List includes name link to Participants page.		
2.17.2	Return Date - Anticipated date with status will change to Active		
2.17.3	Save to Spreadsheet Link - Save to Excel for searching and data formatting.		
2.18	**Cash Report** - Daily Cash Report for the testing site by personnel		
2.18.1	Date - Search by date.		
2.18.2	Shift - Selection of All, AM or PM		
2.18.3	Save to Spreadsheet Link - Save to Excel for searching and data formatting.		
2.19	**Useful Links** - Links to webpages, emails or documents associated with the Program		
2.20	**Search for Participants** - Search by Last, First or both names		
2.21	**Open Receipt** - Supposed to be able to search for a receipt. Often doesn't work, especially for voided receipt. **(Change to Search for Receipt)**	X	
2.22	**Current Participants** - List of Active Participants **(Change title to Active Participants)**	X	
2.22.1	List includes name link to Participants page.		
2.22.2	Date of Birth		
2.22.3	Date and time of last test		
2.22.4	Test Type - Currently lists first test for Participant **(Change to reflect the current test type)**	X	
2.23	**Removed Participants** - Participants who have been temporarily removed		
2.23.1	Same information as Current Participants (2.22.1 thru 2.22.4)		

2.24	**Participants expected to complete the program in 30 days**		
2.24.1	List includes name link to Participants page.		
2.24.2	Scheduled end date - Anticipated last test date		
2.25	**Participants who should have completed the program -** Same information as 2.24 (2.24.1-2.24.2)		
	Header Links		
2.26	**Search for Participants** - Search by Last, First or both names		
2.27	**No Shows** - Same as No Show List (2.1-2.1.2)		
2.28	**New Participan**t - Enrollment page for new Participant		
2.28.1	First Name, Middle Name, Last Name, Jr/Sr, Gender (dropdown box), DOB **(insert selection box)**, County (dropdown box)	X	
2.28.2	Driver's License Information - Number (required unless suspended or revoked), Work Permit Number, check box for Suspended/Revoked		
2.28.3	Primary Address - Required		
2.28.4	Secondary Address - Currently optional		
2.28.5	Contact Info - Phone (Home, Work and Cell), Email Address		
2.28.6	24/7 Program Information		
2.28.7	Type **(Change to Agency)** - Select the entity that placed the individual on the program.	X	
2.28.8	Judge - Select the Judge responsible for placing Participant on the program		
2.28.9	Court Reason - Select the reason placed on the program (Descriptions need clarification)		
2.28.10	Consent Form - **Change to Consent Form Signed: Yes/No dropdown box.** Required.	X	
2.28.11	Start Date - First date of testing. Required		
2.28.12	Scheduled end date - Anticipated last test date		
2.28.13	Offense - Select a specific offense from dropdown box		
2.28.14	Other Offense		
2.28.15	Comment Box - Used for general comments		
2.28.16	Alert Box - Used for important alerts (i.e. Warrant on File). Flashes red at top of Participant's page.		
2.28.17	Employment Information - Employer, address, phone and Supervisor **(add email address box)**	x	
2.29	**Help** - General guide to webpage with links to specific areas. **Expand to a full User's Guide with Frequently Asked Questions/Answers**	X	
2.30	**Logout** - Sign off		
3.0	**Participant's Home Page**		
3.1	**Edit** - Link to Participant's Enrollment Page		
3.2	**Change Status** - Change status to Removed or Completed		
3.3	**Information from Enrollment Page**		
3.4	**State Account** - State Participation Fee Balance **(Change title to State Participation Fee)**	X	
3.4.1	Add a Payment		
3.4.2	Refund Money		
3.4.3	Adjust Balance		
3.4.4	Payment/Refund Info - Date, Description (including link to receipt),		

	Financial info, Recorded By and check box to remove payment/refund due to error		
3.5	**PBT Balance** - View Account - Local financial information. Same info as 3.4.4		
3.6	**U/A Balance** - View Account - Local financial information. Same info as 3.4.4		
3.7	**Drug Patch Balance** - View Account - Local financial information. Same info as 3.4.4		
3.8	**Interlock Balance** - View Account - Local financial information. Same info as 3.4.4		
3.9	**SCRAM Balances** - Local Activation/Deactivation Fees - View Account - Local financial information. Same info as 3.4.4		
3.9.1	SCRAM Activation/Deactivation Fees that stay with Testing Site. **(Change Title to SCRAM Activation/Deactivation)**	X	
3.9.2	SCRAM Daily Fees - Forwarded to AG's Office. **(Change Title to SCRAM Daily Fees)**	X	
3.9.21	Amount to Disburse - $1.00 disbursement back to testing agency for positive balance		
3.9.22	Disbursed - Yes/No		
3.9.23	SCRAM Site - Testing site responsible for SCRAM. Receives disbursement.		
3.10	**Tests** - Lists and manages the testing methods		
3.11	**2xPBT** - Edit link goes to page to waive fees. Remove link removes the test type.		
3.12	**Drug Patch** - Local Activation/Deactivation Fees - View Account - Local financial information. Same info as 3.4.4		
3.13	**Interlock** - Edit link goes to Inspection schedule. Remove link removes the test type.		
3.14	**SCRAM** - Remove link stops daily fees and posts the deactivation fee.		
3.15	**U/A** - Edit link goes to scheduling page to include waiving fees option.		
3.16	**Add Test Type** - Link goes to dropdown box of test types. Adding SCRAM automatically starts daily fees and posts activation fee.		
3.17	**Alert Box** - Used for important alerts (i.e. Warrant on File). Flashes red at top of Participant's page.		
3.18	**Comment Box** - Used for general comments		
3.19	**Option for adding photo**		
3.20	**Option for editing, removing or adding additional Interested Parties**		
3.21	**Documents** - Link to add documents (i.e. Court Orders, Participation Agreements, etc.)		
3.22	**Test Log** - PBT, UA and Interlock Pass/Fail log		
3.23	**Link to Drug Patch Management page.**		
3.23.1	Drug Patch Management page.		
	Recommended Changes from Testing Sites	**Testing Site**	
4.1	Participant List should include Name, DOB and OLN - Used to run Warrant Checks	Minnehaha	
4.2	Add a printable violation report	Minnehaha	
4.3	Add Warrant Affidavit form	Minnehaha	
4.4	No Show List - Ability to sort/view by Test Type	Minnehaha	
4.5	Ability to print multiple receipts for one payment (i.e. $50 payment - print 5 $10.00 receipts). Used as UA tickets.	Minnehaha	

4.6	Add payments directly from the Participant's Home Page	Minnehaha
4.7	Larger button to log test	Minnehaha
4.8	Fingerprint identification	Minnehaha
4.9	Better management of comments on Participants Home Page. Only show recent notes. Archive previous notes.	Minnehaha
4.10	Ability to run missed tests by date	Minnehaha
4.11	Report for SCRAM Daily Fees by date/shift. Same for Activation/Deactivation fees	Minnehaha
4.12	Remove Tester's last name from receipt. Create ID # for tester.	Minnehaha
4.13	U/A and Drug Patch Reports that lists substance	Minnehaha
4.14	Include SCRAM payments/refunds in Cash Report for each shift	Minnehaha
4.15	Give Tester's ability to reactivate all Participants.	Minnehaha
4.16	Phone number fields automatically populate correctly (555) 555-5555	Minnehaha
4.17	Add Court File Number	Butte
4.18	Participant's Name in red bold if they have a negative balance in any account. This would apply to Home Page and any Lists run including them.	Pennington
4.19	Automatically add notice in Alert box for any negative balance.	Pennington
4.20	Updated total of State Participation Fees paid/owed to complete the 30 days ($30.00)	Pennington
4.21	U/As trackable by date in addition to days	Pennington
4.22	Add Involuntary Commitment, Probation and Parole to Offense drop down list.	Lincoln
4.23	Distribute information across page in a manner for easier reading	Pennington
4.24	Tracking mechanism for failed tests for each Participant	Pennington
4.25	Unique Participant ID number separate from the Account numbers. ID number would remain the same throughout 24/7 no matter how many accounts.	
4.26	Show balances on all receipts	Pennington
4.27	Add Attorney General to Court Reason Dropdown	Pennington
4.28	Use Military Time without semi-colon	Minnehaha
4.29	Statistics - Average days on 24/7 Program	
4.30	Automatically change status to removed if no logged test in 7 days.	
4.31	Total days a Participant is on the program (all tests)	
4.32	Receipt should list the type of test.	Minnehaha
4.33	Add ability for U/A test on a monthly basis	Pennington
4.34	Temporary removal automatically posts to No Show List on date scheduled to return	Minnehaha
4.35	Log Testing site and Tester on each test	Brookings
4.36	Ensure fee for test is deducted before payment is logged - create an accurate receipt	Minnehaha
4.37	Ability for testing sites to view all receipts including voided receipts	
4.38	All data from current website transferred to new website	
4.39	Only enrolling site can change the status of a Participant	Brookings
4.40	Add new test type for Mobile Breath Alcohol Testing Device. Should be set up similar to SCRAM	
5.0	**Administrative Page**	

5.1	**Combine Participants Link** - Combines accounts when a new account is made in error. **(Change title to Combine Accounts)**	
5.1.1	Enter accounts number to keep and the one to remove.	
5.1.2	Combine Participants link moves data from the "Remove" account to the "Keep" account then deletes the "Remove" account	
5.2	**Manage Users Link** - Adds Users/Testers to the Program	
5.2.1	Search by Testing Site and User	
5.2.2	Dropdown box to select testing site	
5.2.3	Page displays Name, Username, Phone, Email	
5.2.4	Edit -Link take you to the User's information page	
5.2.5	New User Link - Used by admin to add a new User.	
5.2.6	New User enrollment page	
5.2.7	Site - Select Testing Site	
5.2.8	Username	
5.2.9	Type - Provides type of access (Normal, Supervisor, Admin) **(Add Read Only Access)**	
5.2.10	Name Info.	
5.2.11	Contact Info.	
5.3	**Manage Agency User Link** - Gives specific agencies access to entire state 24/7 data base.	
5.4	**Manage Judges Link** - List of Judges available for testing sites to select.	
5.4.1	Edit Link - Used to remove Judge from list or move to another court.	
5.4.2	New Judge Link - Used to add new Judge to the list	
5.4.3	New Judge Page - Enter Name and Circuit	
5.5	**Manage Sites Link** - List of approved testing sites	
5.5.1	Edit Link - Goes to site's information page	
5.5.2	New Site Link - Used to add a new testing site.	
5.5.3	New Site Info Page	
5.6	**Manage Testing Fees Link** - Ability to change the testing fees for specific test types. Applied from change forward (no change to previous charges)	
5.6.1	Test Type - Search by specific test type.	
5.6.2	Enter new fees	
5.7	**State Disbursements Link** - State Participation Disbursements from testing sites. **(Change to State Participation Fee Disbursements)**	
5.7.1	From/To - Defaults to the last 3 months. Capable of searching any duration or specific timeframe.	
5.7.2	Date, Site and Amount	
5.7.3	Remove Link - Allows administrator to remove the payment from this page and the agency's State Account Disbursement page	
5.7.4	Approve Link - Allows administrator to confirm payment when received.	
5.7.5	Save to Spreadsheet Link - Save to Excel for searching and data formatting.	
	SCRAM	
5.8	**County to State SCRAM Disbursement** - Lists Unreceived and Undisbursed SCRAM payments.	
5.8.1	Unreceived Disbursements - Payments submitted or mailed by agency	

	but not yet received by AG	
5.8.2	Site Name, Status, Date/time posted and Amount	
5.8.3	View Link - Goes to page with specific details regarding that payment	
5.8.4	Change Status Link - Changes payment to Received.	
5.8.5	Undisbursed Payments - SCRAM payments collected at testing site but not forwarded to AG.	
5.8.6	View Link - Goes to page with specific details regarding that payment	
5.8.7	Received Payments - List of all SCRAM payments received by AG from testing sites.	
5.8.8	From/To - Defaults to the last year. Capable of searching any duration or specific timeframe.	
5.8.9	View Link - Goes to page with specific details regarding that payment	
5.9	**State to County SCRAM Disbursements** - Used to determine Quarterly SCRAM Allocations returned to testing agency	
5.9.1	Agency Name Link - Goes to page with specific SCRAM disbursement details for that agency.	
5.9.2	Balance Due (Based on SCRAM payments received from testing site. $1.00 per day per active bracelet with a positive account balance.)	
5.9.3	Add a Disbursement - Completed by Administrator when disbursement is paid	
5.9.4	Add a Balance Adjustment - Completed by Administrator when necessary	
5.9.5	Daily activity including earned allocation and current balance. Also includes disbursements when paid.	
5.9.6	View Link - Goes to page with specific details for the allocation/disbursement for that date.	
5.10	**SCRAM Account Status Link** - Used by Administrator to monitor SCRAM balances and initiate action to collect delinquent accounts	
5.10.1	Site - Select Testing Site	
5.10.2	Balance - Search by All, Negative, Positive and Zero	
5.10.3	Search by Active/Inactive/All	
5.10.4	Delinquency - Search by Non-Delinquent, Delinquent, All	
5.10.5	Payment Plan - Search by Weekly, Bi-Weekly, Monthly	
5.10.6	Action Needed -Yes/No	
5.10.7	Name Link - Goes to page with specific details	
5.10.8	Change Status	
5.10.9	Change Payment Plan	
5.11	**SCRAM County Disbursement Start Dates Link** - SCRAM Quarterly Allocation starting dates for each agency. Agency Link - Goes to setting date page.	
5.11.1	Set starting date for agency. Current date automatically fills. Can be manually changed.	
5.12	**SCRAM Fee Gaps Link** - Used by Administrator to fill in system wide missing SCRAM Daily Fees (used when system offline at time of daily fee auto logging)	
5.12.1	Date Range - Used to search for missing SCRAM Daily Fees.	
	Reports	
5.13	**Participants Link** - Goes to page to search Participants	

5.13.1	Dropdown box to select Testing Site	
5.13.2	Dropdown box to select test type, Judge, Agency, Offense or Status	
5.13.3	Save to Spreadsheet Link - Save to Excel for searching and data formatting.	
5.14	**Daily Activity Link** - Goes to page with specific testing details by date and testing site.	
5.14.1	From/To - Defaults to the last month. Capable of searching any duration or specific timeframe.	
5.14.2	Dropdown box to select Testing Site	
5.14.3	Save to Spreadsheet Link - Save to Excel for searching and data formatting.	
5.15	**Fees Earned Link** - Local fees collected for the local agency 24/7 Program fund.	
5.15.1	From/To - Defaults to the last month. Capable of searching any duration or specific timeframe.	
5.15.2	List by Agency includes 1xPBt, 2xPBT, UA and Drug Patch **(Add Ignition Interlock and SCRAM Allocations)**	
5.15.3	Save to Spreadsheet Link - Save to Excel for searching and data formatting.	
5.16	**Duplicate Fees and Payments Link** - Goes to page that displays possible duplicate SCRAM Fees and Payments	
5.16.1	From/To - Defaults to the last day. Capable of searching any duration or specific timeframe.	
5.16.2	Possible Duplicate SCRAM Fees	
5.16.3	Possible Duplicate SCRAM Payments	
5.16.4	Name Link - Goes to Participants SCRAM pages (Activation/Deactivation and Daily Fees depending on location of possible duplication)	
5.17	State Fees Owed Link - Goes to page displaying State Participation Fees owed.	
5.18	**Test Stats Link** - Statistics for the 24/7 Program. Automatically loads from starting date of program to current date **(Eliminate automatic search)**	
5.18.1	From/To - Defaults to starting date of program to current date. Capable of searching any duration or specific timeframe. **(Change starting date)**	
5.18.2	Dropdown box to select All or specific testing site.	
5.18.3	PBT Stats - Includes 1xPBT and 2xPBT	
5.18.4	U/A Stats	
5.18.5	Drug Patch Stats	
5.18.6	Save to Spreadsheet Link - Save to Excel for searching and data formatting.	
5.19	**Action Log Link** - List of daily programming runs	
5.19.1	From/To - Defaults to the last month. Capable of searching any duration or specific timeframe.	
5.19.2	List of programming run details.	
5.20	**Records Pending Removal Lin**k - Administrator approves all removals from the program. Link goes to page with specific details of each removal.	
5.21	Switch to Site Link - Goes to selected testing site's main page as Administrator	

5.22	**Disaster Recover**	
5.22.1	A disaster recovery plan will need to be implemented if the solution is Vendor hosted.	
5.22.2	A disaster recovery should bring the system back up within 12 hours.	

Log In

Main Page

24/7 Program

Brookings - John Doe

2.0 Main | 2.26 Search | 2.27 No Shows | 2.28 New Participant | 2.29 Help | 2.30 Logout

Site Administration

List No Shows 2.1
Add Existing Participant 2.2
Calibrations Remove
State Account Disbursements 2.3
SCRAM Payments to Disburse 2.4
SCRAM Disbursements 2.5

Change Password 2.6
Manage Users 2.7

Reports

Account Activity 2.8
Participants 2.9
Repeat Participants 2.10
SCRAM Days 2.11
SCRAM Participants 2.12
Summary 2.13
Officer Test Counts 2.14
Unpaid Fees 2.15
Unpaid SCRAM Fees 2.16
Temporary Removals 2.17
Participants Without Interested Parties Remove
Cash Report 2.18

Mental Health Screening Remove

Search / Add Remove

Useful Links 2.19

SCRAM
SCRAM Supplies
Intoximeter Supplies
Forms/Documents
24/7 Listserv
24/7 County Contact List
CPS Contact Numbers
Intoxalock Service Centers

SCRAM Customer Support
(303) 785-7879
support@alcoholmonitoring.com

For assistance, please contact John Doe
John.Doe@state.sd.us
(605) 555-5555

Search Participants 2.20

Last | First | Search

Open Receipt 2.21

Receipt # | Search

Current Participants 2.22

Name 2.22.1	2.22.2 DOB	Last Tested 2.22.3	Type 2.22.4
Smith, John J	9/29/1995	09/29/2016 15:33	SCRAM
Smith, John Jacob	1/29/1995	10/28/2016 09:24	U/A
Smith, Jane A	5/20/1975	10/29/2016 07:12	2x PBT
Smith, Jane Ann	6/18/1990	08/03/2016 14:33	SCRAM

Removed Participants 2.23

2.23.1

Name	DOB	Last Tested	Type
Smith, John J	10/26/1983	08/11/2015 12:50	2x PBT
Smith, John Jacob	12/1/1985	05/15/2011 22:05	2x PBT
Smith, Jane A	7/18/1989	09/18/2015 20:48	2x PBT

Participants expected to complete the program with 30 days 2.24

Name 2.24.1	Scheduled End Date 2.24.2
Smith, John J	11/16/2016
Smith, John Jacob	11/24/2016

Participants who should have completed the program 2.25

Name	Scheduled End Date
Smith, Jane A	04/27/2016
Smith, Jane Ann	06/01/2016
Smith, John J	06/07/2016

No Show List

24/7 Program

Brookings - John Doe Main Search No Shows New Participant Help Logout

Quick Links
Sat AM A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Fri PM A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

2.1.1

Missed Tests
For Sat AM

Name	Test	Balance		
Smith, John J	2x PBT	$2.00	Add No-Show	Add Excused
Smith, John Jacob	2x PBT	$0.00	Add No-Show	Add Excused

2.1.2

Missed Tests
For Fri PM

	Test	Balance		
Smith, John J	2x PBT	$2.00	Add No-Show	Add Excused
Smith, John Jacob	U/A	$0.00	Add No-Show	Add Excused

Add Existing Participant

24/7 Program

Brookings - John Doe Main Search No Shows New Participant Help Logout

Add Existing Participant 2.2

Please enter the participant ID (eg. 'NJEG-T5XZ') below to add a participant from another site to your site's list of participants.

2.2.1 Add Participant

State Account Disbursements

24/7 Program

Brookings - John Doe

Main Search No Shows New Participant Help Logout

State Account Disbursements
Brookings

Add a Disbursement 2.3.1

Amount

Date 10/29/2016 09:16

Comments

Add Disbursement

From 07/31/2016

To 10/29/2016

2.3.2

update

2.3.3

Date	State Fees	Unpaid Fees	Collected Fees	Disbursements	Balance	
10/29/2016	$3.00	$2.00	$1.00	$0.00	$60.00	View 2.34
10/28/2016	$5.00	$1.00	$4.00	$0.00	$59.00	View
10/27/2016	$6.00	$1.00	$5.00	$0.00	$55.00	View
Totals:	$605.00	$8.00	$597.00	$640.00		

Total State Fees	$605.00
- Total Unpaid	$8.00
Collected State Fees:	$597.00
- Total Disbursed	$640.00
Balance Change	($43.00)
+ Balance Forward	$103.00
New Balance	$60.00

2.3.5

SCRAM Payments to Disburse

24/7 Program

Brookings - John Doe

Main Search No Shows New Participant Help Logout

SCRAM Payments to Disburse 2.4

Brookings

Add a Disbursement

Amount $1,520.00

Date

Comments

2.4.1

Add Disbursement

To 10/29/2016 2.4.2

update

Name		Posted	Date	Amount	Receipt Number
Smith, John J	2.4.3	10/17/2016 12:14	10/17/2016	$42.00	Receipt #18740
Smith, John Jacob		10/24/2016 17:02	10/24/2016	$40.00	Receipt #18858

SCRAM Disbursements

24/7 Program

Brookings - John Doe

Main Search No Shows New Participant Help Logout

SCRAM Disbursements 2.5

Brookings

From 10/29/2015

To 10/29/2016

2.5.1

update

Status 2.5.2	Posted	Date	Amount	
Undisbursed			$1,520.00	View 2.5.3
Unreceived	10/17/2016 14:04	10/17/2016	$2,039.00	View
Voucher for $2,039.00 turned in to Brookings County Finance Office for this payment to the SD AG Office. (John Doe)				
Received	10/05/2016 16:03	10/05/2016	$2,802.00	View
Voucher for $2,802.00 turned in to Brookings County Finance Office for this payment to the SD AG Office. (John Doe)				
Received	09/23/2016 11:22	09/23/2016	$1,910.00	View
Voucher for $1,910.00 turned in to Brookings County Finance Office for this payment to the SD AG Office. (John Doe)				

Total Undisbursed:	$1,520.00
Total Unreceived:	$2,039.00
Total Received:	$51,975.00

Account Activity

24/7 Program

Brookings - John Doe

Main Search No Shows New Participant Help Logout

Account Activity 2.8

Date 10/29/2016 2.8.1

Shift All 2.8.2

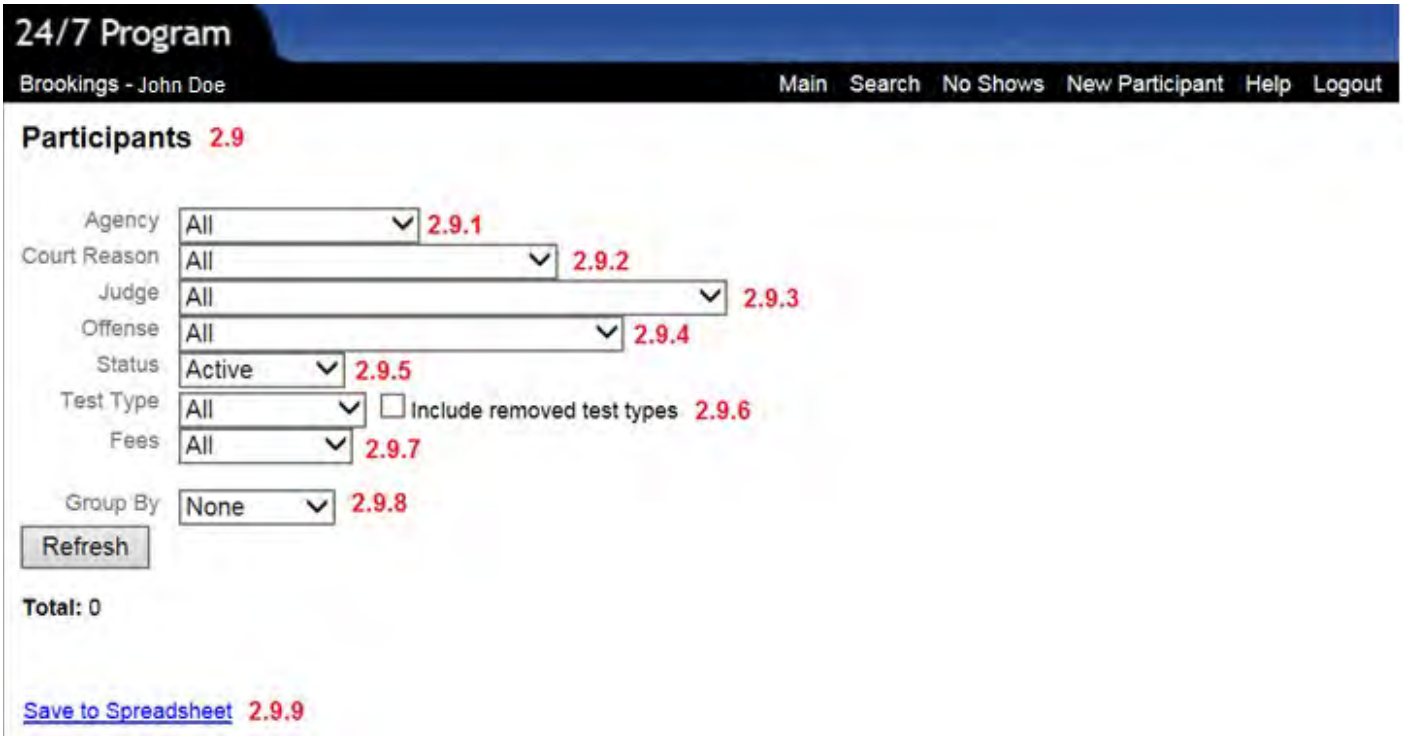
Type All 2.8.3

Details All 2.8.4

Date	Participant			Fee	Payment	Bal Adj	Recorded By
10/29/2016 01:16	Smith, John J	2x PBT	Passed	$1.00			John Doe
10/29/2016 02:19	Smith, John Jacob	2x PBT	Passed	$1.00			Jane Doe
10/29/2016 05:29	Smith, Jane A	2x PBT	Passed	$1.00			John Doe
10/29/2016 05:52	Smith, Jane Ann	2x PBT	Passed	$1.00			Jane Doe
10/29/2016 06:17	Smith, John J	2x PBT	Passed	$1.00			John Doe
10/29/2016 06:20	Smith, John Jacob	2x PBT	Passed	$1.00			Jane Doe
10/29/2016 06:20	Smith, Jane A	2x PBT	State Fee	$1.00			
10/29/2016 06:25	Smith, Jane Ann	2x PBT	Passed	$1.00			Jane Doe
10/29/2016 06:34	Smith, John J	2x PBT	Passed	$1.00			John Doe
10/29/2016 06:38	Smith, John Jacob	2x PBT	Passed	$1.00			Jane Doe
will blow 3 times today							
10/29/2016 06:42	Smith, Jane A	2x PBT	Passed	$1.00			John Doe
10/29/2016 06:44	Smith, Jane Ann	2x PBT	Passed	$1.00			Jane Doe
10/29/2016 06:48	Smith, John J	2x PBT	Passed	$1.00			John Doe
10/29/2016 06:48	Smith, John Jacob	2x PBT	State Fee	$1.00			
10/29/2016 06:53	Smith, Jane A	2x PBT	Passed	$1.00			John Doe
10/29/2016 07:21	Smith, Jane Ann	2x PBT	Passed	$1.00			Jane Doe
10/29/2016 07:36	Smith, John J	2x PBT	Passed	$1.00			John Doe
10/29/2016 08:04	Smith, John Jacob	2x PBT	Passed	$1.00			Jane Doe
10/29/2016 08:28	Smith, Jane A	2x PBT	Passed	$1.00			John Doe
10/29/2016 08:32	Smith, Jane Ann	2x PBT	State Fee	$1.00			
10/29/2016 08:54	Smith, John J	2x PBT	Passed	$1.00			John Doe
10/29/2016 11:53	Smith, John Jacob	2x PBT	Passed	$1.00			Jane Doe
Totals:				**$22.00**	**$0.00**	**$0.00**	

Save to Spreadsheet

Participants



Repeat Participants

SCRAM Days

24/7 Program

Brookings - John Doe

Main Search No Shows New Participant Help Logout

SCRAM Days 2.11

From 9/1/2016
To 9/30/2016

2.11.1

Participant	SCRAM Site	SCRAM Days
Smith, John J	Brookings	2
Smith, John Jacob	Brookings	30
Smith, Jane A	Brookings	15
Smith, Jane Ann	Brookings	30
Smith, John J	Brookings	30
Smith, John Jacob	Brookings	30
Smith, Jane A	Brookings	30
Smith, Jane Ann	Brookings	30
Smith, John J	Brookings	1
Smith, John Jacob	Brookings	30
Smith, Jane A	Brookings	30
Smith, Jane Ann	Brookings	30
Smith, John J	Brookings	30
Smith, John Jacob	Brookings	30
Smith, Jane A	Brookings	30
Smith, Jane Ann	Brookings	30
Smith, John J	Brookings	22
Smith, John Jacob	Brookings	9
Smith, Jane A	Brookings	2
Smith, Jane Ann	Brookings	20
Smith, John J	Brookings	30
Smith, John Jacob	Brookings	30
Smith, Jane A	Brookings	12
Smith, Jane Ann	Brookings	30
Smith, John J	Brookings	30
Smith, John Jacob	Brookings	25
Smith, Jane A	Brookings	26
Smith, Jane Ann	Brookings	12
Smith, John J	Brookings	30

2.11.2

Total: 892

Save to Spreadsheet

SCRAM Participants

24/7 Program

Brookings - John Doe

Main Search No Shows New Participant Help Logout

SCRAM Participants 2.12

2.12.1

SCRAM Site	Client	Checkout	Checkin	Total Billed	Total Paid Clerk	Total Paid DOC	Balance Remove
Brookings	John Jacob Smith	03/25/2010	09/28/2010	($1,128.00)	$1,128.00	$0.00	$0.00
Brookings	John Jacob Smith	12/20/2010	03/14/2011	($510.00)	$510.00	$0.00	$0.00
Brookings	Jane Ann Smith	11/01/2011	12/06/2011	($216.00)	$220.00	$0.00	$4.00
Brookings	Jane Ann Smith	09/08/2015	07/27/2016	($1,944.00)	$1,944.00	$0.00	$0.00

Summary Report

24/7 Program

Brookings - John Doe

Main Search No Shows New Participant Help Logout

Summary Report 2.13

From 10/28/2016 ×

To 10/29/2016

2.13.1

Show Days 2.13.2

Test Type All 2.13.3

Agency All 2.13.4

Court Reason All 2.13.5

Refresh

2.13.6	# Part	# Tests Given	# Failed	Earned	Scram (DPS) Fees	State Fees	Collected	Refunded	# pre-trial	# pre-sent.	# post-sent.	# cond. of sent.
10/28/2016	1615	47	0	$140.00	$0.00	$5.00	$128.00	$9.00	546	38	112	640
10/29/2016	1615	19	0	$19.00	$0.00	$3.00	$0.00	$0.00	546	38	112	640
Totals		**66**	**0**	**$159.00**	**$0.00**	**$8.00**	**$128.00**	**$9.00**	**1092**	**76**	**224**	**1280**

Save to Spreadsheet 2.13.7

Officer Test Counts

24/7 Program

Brookings - John Doe

Main Search No Shows New Participant Help Logout

Officer Test Counts 2.14

From 9/1/2016
To 9/30/2016

2.14.1

Testing Officer	Total PBT	Total 1x PBT	Total 2x PBT	Total UA
6A14	4	0	4	0
6A30	4	0	4	0
6A9	3	0	3	0
aah	69	0	69	1
agl	33	0	33	3
AJE	64	0	64	7
ajohnson	0	0	0	1
ajs	55	0	55	1
ALK	61	0	61	2
Jane Doe	0	0	0	0

Save to Spreadsheet 2.14.2

Unpaid Fees

24/7 Program

Brookings -John Doe

Main Search No Shows New Participant Help Logout

Agency All 2.15.1

Court Reason All 2.15.2

Judge All 2.15.3

Offense All 2.15.4

Test Type All ☐ Include removed test types 2.15.5

Refresh

Unpaid Fees (Active Participants) on 10/29/2016

Participant	Agency	Interested Parties	PBT	U/A	Interlock	Drug Patch	Scram (Dps)	Scram	State Fees	Total
Smith, John	Court		$1.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$1.00
Smith, John	DOC	DOE, JANE (Parole Officer)	$0.00	$23.00	$0.00	$0.00	$0.00	$0.00	$1.00	$24.00
Smith, Jane	Court		$1.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$1.00
Smith, Jane	Court	DOE, JANE (Probation Officer)	$0.00	$0.00	$0.00	$213.00	$0.00	$0.00	$0.00	$213.00
Smith,	Court		$0.00	$0.00	$0.00	$128.00	$0.00	$0.00	$0.00	$128.00

Save to Spreadsheet 2.15.6

Unpaid SCRAM Fees

24/7 Program

Brookings - John Doe

Main Search No Shows New Participant Help Logout

Agency All 2.16.1

Court Reason All 2.16.2

Judge All 2.16.3

Offense All 2.16.4

Refresh

Unpaid SCRAM Fees (Active Participants) on 10/29/2016

SCRAM Site	Participant	Agency	Interested Parties	Unpaid Fees
Brookings	Smith, John J	Court	JESSICA PAGE (Probation Officer)	$122.00
Brookings	Smith, John Jacob	Court		$23.00

Total: $145.00

Unpaid SCRAM Fees (Inactive Participants) on 10/29/2016

SCRAM Site	Participant	Agency	Interested Parties	Unpaid Fees
Brookings	Smith, Jane A	Court		$85.00
Brookings	Smith, Jane Ann	Court		$360.00
Brookings	Smith, John J	Court		$90.00
Brookings	Smith, John Jacob	Court		$382.70
Brookings	Smith, Jane A	Court		$50.00
Brookings	Smith, Jane Ann	Court		$525.00
Brookings	Smith, John J	Court		$320.00
Brookings	Smith, John Jacob	Court		$65.00
Brookings	Smith, Jane A	Court	JOHN DOE (Judge)	$108.00
Brookings	Smith, Jane Ann	Court		$225.00

Total: $2,210.70

Save to Spreadsheet 2.16.5

Temporary Removals

24/7 Program

Brookings - John Doe

Main Search No Shows New Participant Help Logout

Temporary Removals 2.17

2.17.1 Name	2.17.2 Return Date
Smith, John J	08/13/2013
Smith, John Jacob	12/29/2015

Save to Spreadsheet 2.17.3

Cash Report

24/7 Program

Brookings - John Doe

Main Search No Shows New Participant Help Logout

Cash Report 2.18

Date 10/28/2016 2.18.1

Shift All 2.18.2

Refresh

User	PBT	U/A	Drug Patch	Interlock	SCRAM (DPS)	SCRAM	State Fees	Total
Smith, John	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Smith, Jane	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Smith, John Jacob	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Smith, Jane A	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Smith, John	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Smith, Jane	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Smith, John Jacob	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Smith, Jane A	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Smith, John	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Smith, Jane	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Smith, John Jacob	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Smith, Jane A	$14.00	$12.00	$0.00	$0.00	$0.00	$40.00	$33.00	**$99.00**
Smith, John	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Smith, Jane	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Smith, John Jacob	$0.00	$20.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$20.00**
Totals:	**$14.00**	**$32.00**	**$0.00**	**$0.00**	**$0.00**	**$40.00**	**$33.00**	**$119.00**

Save to Spreadsheet 2.18.3

Search for Participants

24/7 Program

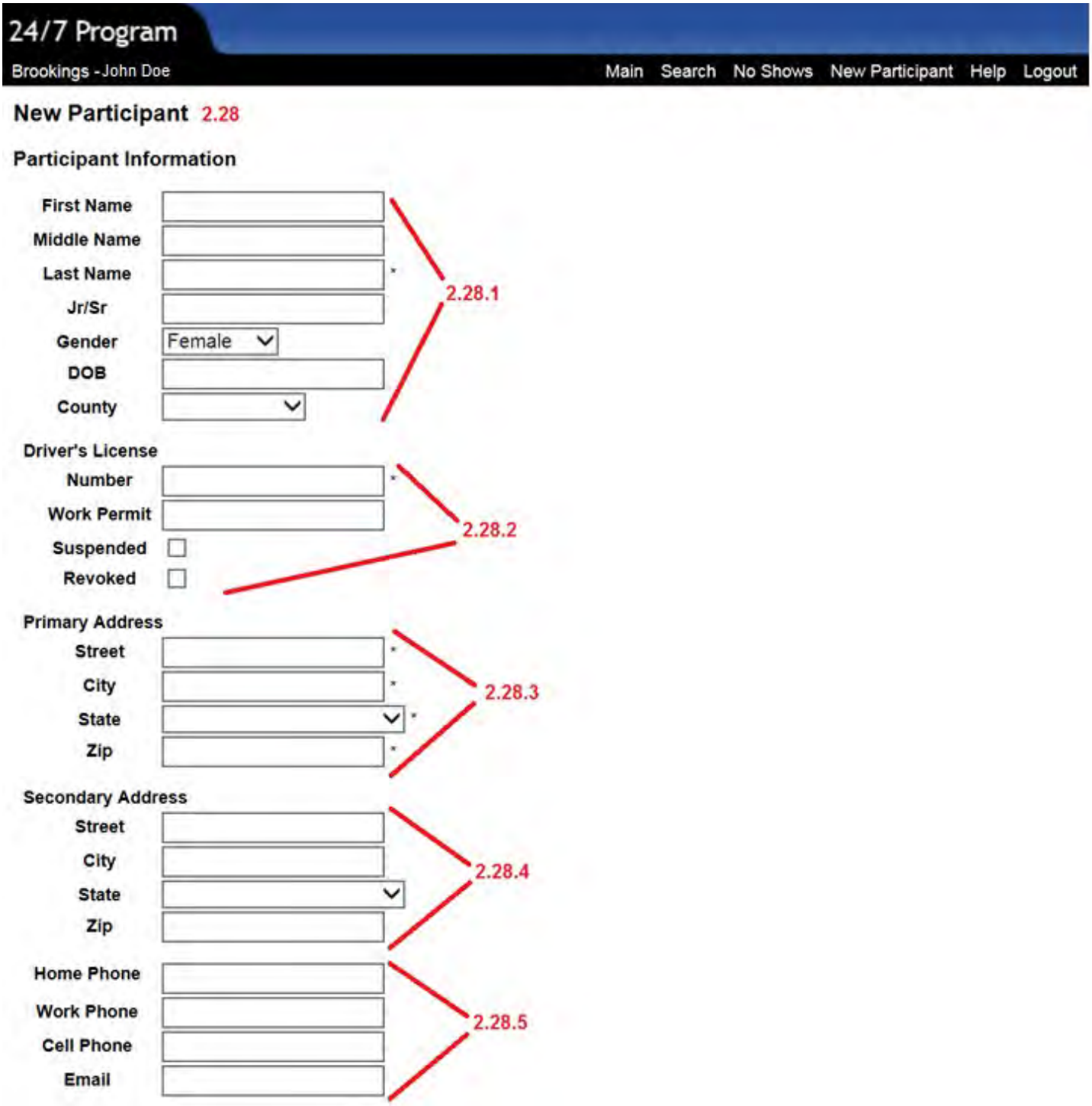
Brookings - John Doe

Main Search No Shows New Participant Help Logout

Search Participants 2.26

Last | First | Participant # | Search

New Participant (Enrollment Page)



New Participant (Enrollment Page) - Continued

A

24/7 Program Information 2.28.6

Type	Court	2.28.7
Judge	Fifth Judicial Circuit - John Doe	2.28.8
Court Reason	Unknown	2.28.9
Consent Form		*2.28.10
Start Date		* 2.28.11
Scheduled End Date		2.28.12
Offense	Abuse and Neglect	2.28.13
Other Offenses		2.28.14
Comments	2.28.15	
Alert	2.28.16	

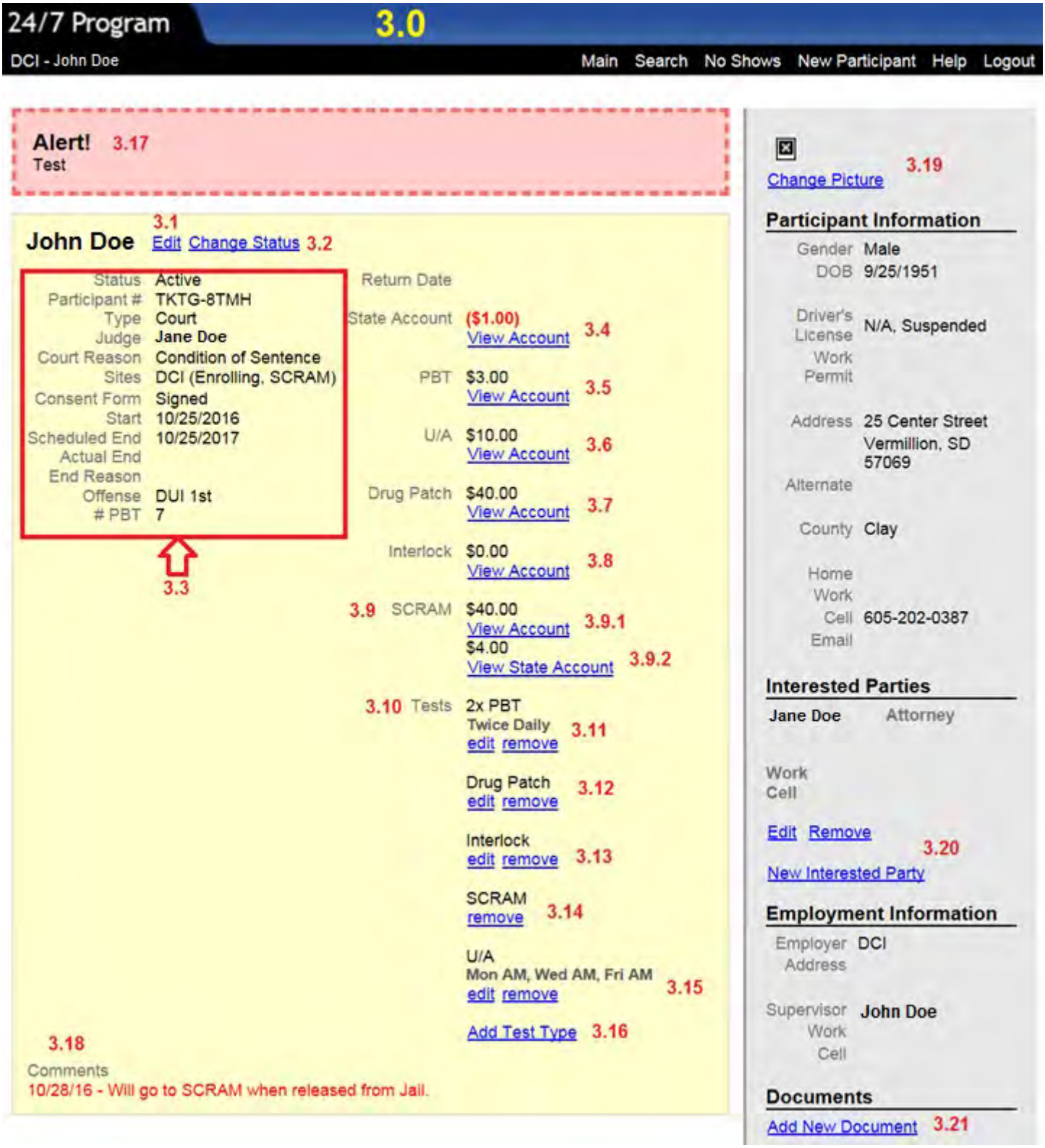
Employment Information

Employer	
Street	
City	
State	
Zip	
Supervisor	
Work Phone	
Cell Phone	

2.28.17

Add Cancel

Participant's Home Page



Participant's Home Page - Continued

Test Log

Test	2x PBT	**Result**	Passed
Date	10/29/2016 12:42		
Testing Officer			
PBT Value			
Comments			
Payment			

Log Test
Manage Drug Patches 3.23

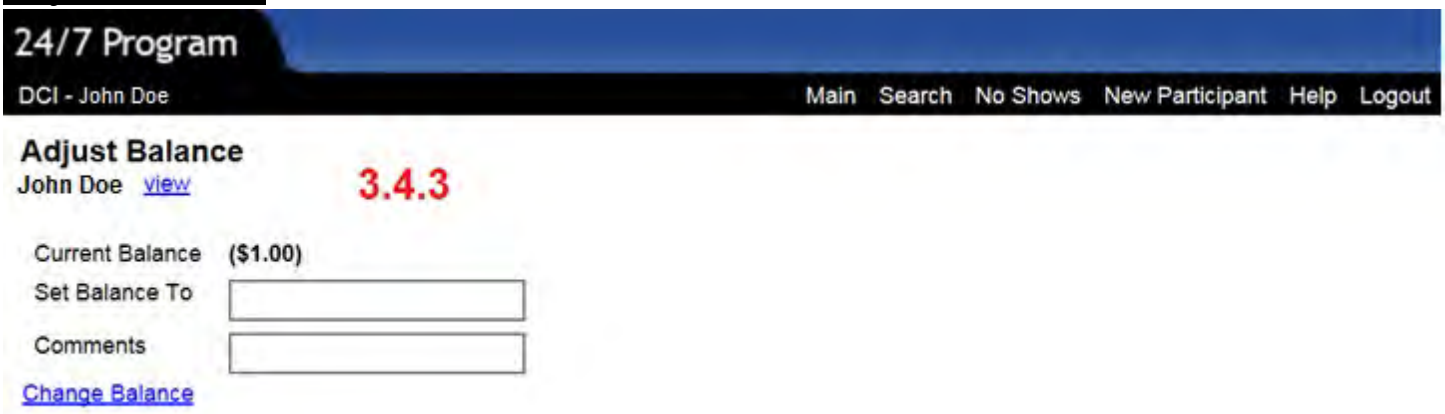
3.22

Date	Type	Result	Testing Officer	PBT Value	Fee	
10/29/2016 12:14	Interlock	Activation Fee	John Doe		$40.00	remove
10/29/2016 11:53	SCRAM	Activation Fee	John Doe		$40.00	remove
10/28/2016 12:00 Jail	2x PBT	Excused			$0.00	remove
10/27/2016 17:00	2x PBT	Passed	JD		$1.00	remove
10/27/2016 8:00	2x PBT	Passed	JD		$1.00	remove
10/27/2016 8:00	2x PBT	State Fee			$1.00	
10/26/2016 17:00	2x PBT	Passed	JD		$1.00	remove
10/26/2016 17:00	2x PBT	Passed	JD		$1.00	remove
10/26/2016 8:00	2x PBT	Passed	JD		$1.00	remove
10/26/2016 8:00	2x PBT	State Fee			$1.00	
10/25/2016 17:00	2x PBT	Passed	JD		$1.00	remove
10/25/2016 8:00	2x PBT	Passed	JD		$1.00	remove
10/25/2016 8:00	2x PBT	State Fee			$1.00	

Show All...

State Participation Fee Account (Same info for PBT, U/A, Drug Patch, Interlock and SCRAM Activation/Deactivation

Adjust Balance



SCRAM Activation/Deactivation

24/7 Program

DCI - John Doe

Main Search No Shows New Participant Help Logout

Account History

John Doe view

3.9.1

SCRAM site: DCI

Add a Payment

Amount

Date 10/29/2016 13:21

Comments

Add Payment

Refund Money

Amount

Date 10/29/2016 13:21

Comments

Refund Money

Adjust Balance

Date			Fee	Payment	Adjustment	Balance	Recorded By	Check All
10/29/2016 11:55	Payment	Print Receipt #1156		$80.00		$40.00	John Doe	☐
10/29/2016 11:53	SCRAM	Activation Fee	$40.00			($40.00)	John Doe	☐

Remove

Show All

SCRAM Daily Fees

24/7 Program

DCI - John Doe

Main Search No Shows New Participant Help Logout

SCRAM State Account

John Doe view

3.9.2

SCRAM site: DCI 3.9.23

Add a Payment

Amount

Type Payment

Date 10/29/2016 13:24

Comments

Add Payment

Date			Fee	Payment	Balance	Amount to Disburse	Disbursed	Check All
10/29/2016	Payment	Print Receipt #1157		$10.00	$4.00		No	☐
DCI						3.9.21	3.9.22	
10/29/2016	Fee		$6.00		($6.00)	$1.00	No	☐
DCI								

Remove

Managing Drug Patches

24/7 Program

DCI - John Doe | Main | Search | No Shows | New Participant | Help | Logout

Manage Drug Patches 3.23.1

John Doe view

Patch #	
Applied At	10/29/2016 13:45
Remove At	
Payment	
Comments	

Add Patch

Administrative Page

24/7 Program 5.0

DCI - Administrator | Main | Admin | Search | No Shows | New Participant | Help | Logout

Combine Participants 5.1
Manage Users 5.2
Manage Agency Users 5.3
Manage Judges 5.4
Manage Sites 5.5
Manage Testing Fees 5.6

State Disbursements 5.7

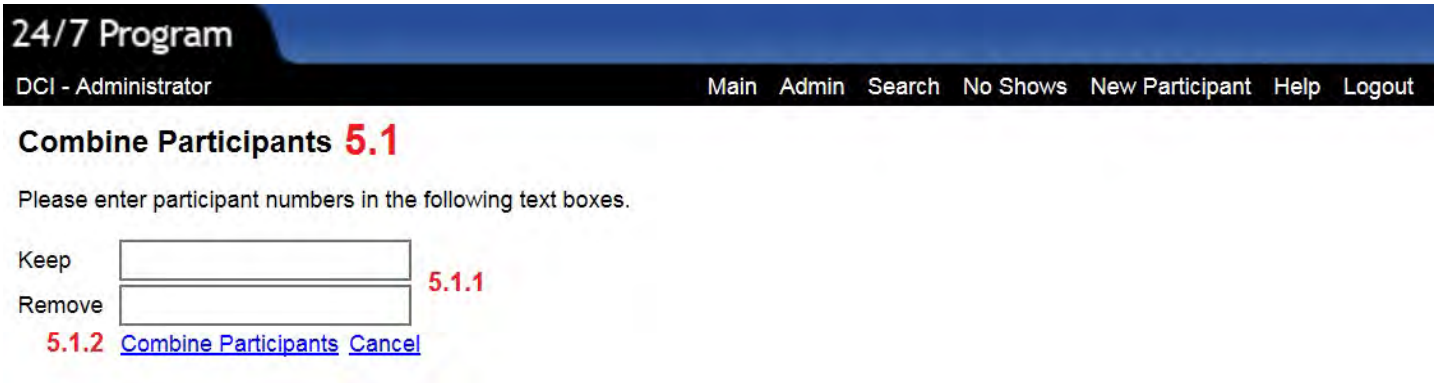
Scram
County to State Scram Disbursements 5.8
State to County Scram Disbursements 5.9
Scram Account Statuses 5.10
Scram County Disbursement Start Dates 5.11
Scram Fee Gaps 5.12

Reports
Participants 5.13
Daily Activity 5.14
Fees Earned 5.15
Duplicate Fees and Payments 5.16
State Fees Owed 5.17
Test Stats 5.18
Action Log 5.19

Record Removal Requests
There are records pending removal 5.20

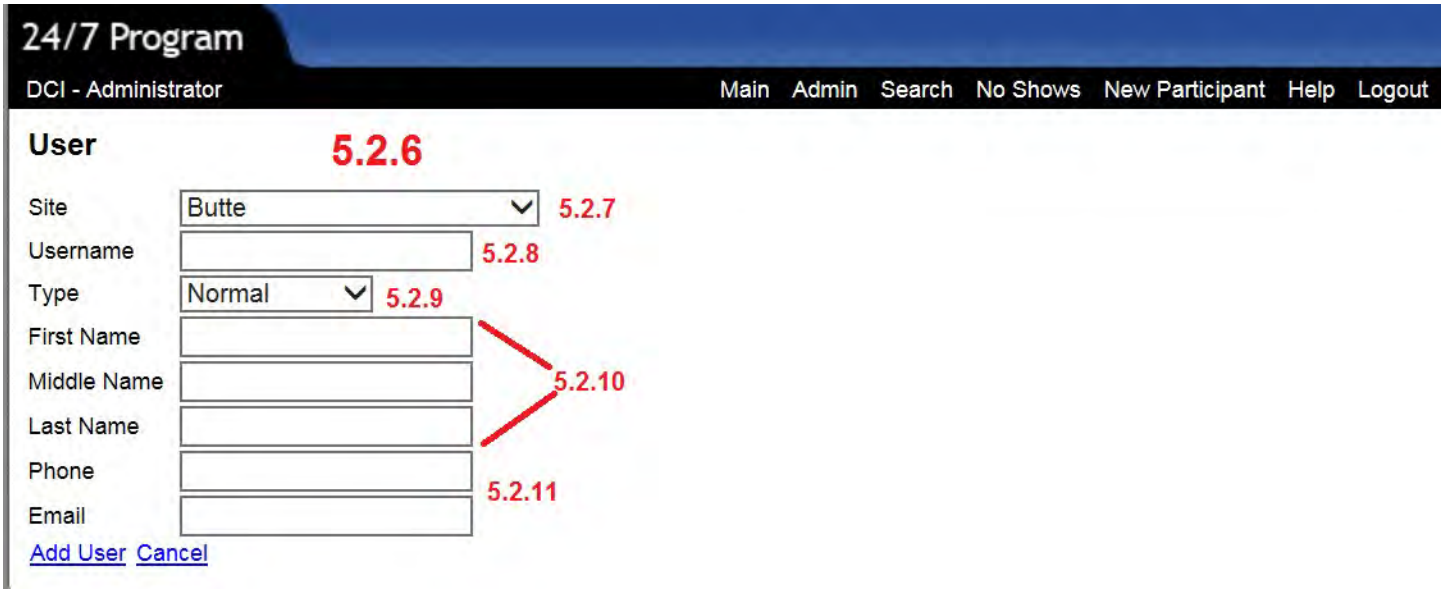
Armour PD | Switch to Site 5.21

Combine Participants



Manage Users

New User Enrollment Page



Manage Agency Users

24/7 Program

DCI - Administrator

Main Admin Search No Shows New Participant Help Logout

Agency Users

5.3

Court

Name	Username	
John Doe	courtservices	edit
John Doe	jdoe	edit
Clay County	claycounty	edit
Edmunds County	edmundscounty	edit
John Doe	jdoe	edit
jf test	jftest	edit
John Doe ion	jdoe	edit
Lincoln County	lincolncounty	edit
Meade County	Meadecounty	edit
Minnehaha County	MinnehahaCounty	edit
Pennington County	penningtoncounty	edit
John Doe	jdoe	edit
Union County	unioncounty	edit

New User

Manage Judges

24/7 Program

DCI - Administrator

Main Admin Search No Shows New Participant Help Logout

Manage Judges

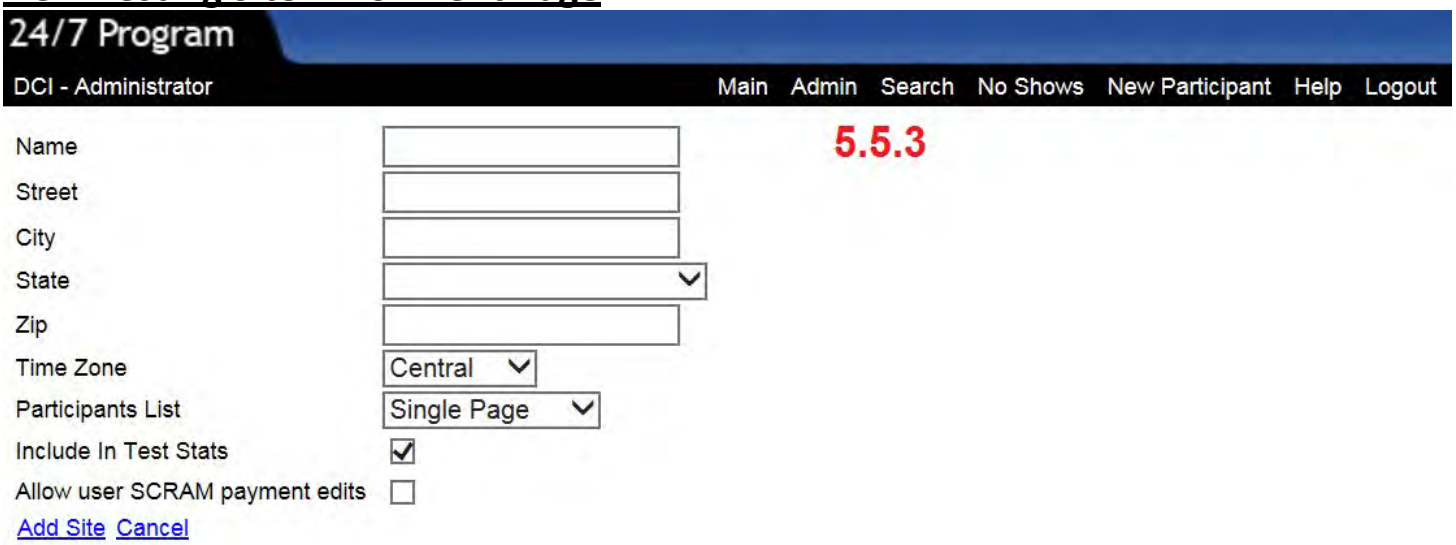
5.4

Name	
John J Doe	edit 5.4.1
Jane A Doe	edit
John Doe	edit
John J Doe	edit
Jane A Doe	edit
John Doe	edit
John J Doe	edit
Jane A Doe	edit
John Doe	edit
John J Doe	edit
Jane A Doe	edit
John Doe	edit
John Doe	edit
John J Doe	edit
Jane A Doe	edit
John Doe	edit
John Doe	edit

New Judge 5.4.2

Manage Sites

New Testing Site Enrollment Page



Manage Testing Fees

24/7 Program

DCI - Administrator

Main Admin Search No Shows New Participant Help Logout

Manage Testing Fees 5.6

---------- 5.6.1

5.6.2

Activation Fee: $

Deactivation Fee: $

Testing Fee: $ The total amount owed by the participant for a single test, or for a day of SCRAM testing.

State Daily Fee: $

State Daily Cap: $ A Cap of 0 means unlimited charges.

Save Cancel

State Disbursement

24/7 Program

DCI - Administrator

Main Admin Search No Shows New Participant Help Logout

From 10/15/2016

To 10/30/2016

update 5.7.1 5.7

Date	Site	Amount		
10/17/2016 14:05	Brookings	$119.00	Approve	Remove
Voucher for $119.00 turned in to the Brookings County Finance Office for this payment to the SD AG Office. (Jane Doe)				
10/19/2016 10:49	Roberts	$284.00		Remove 5.7.3
Received and entered by John				
10/20/2016 15:04	Beadle	$443.00		Remove
Received and entered by John				
10/24/2016 11:06	Hughes	$898.00		Remove
Received and entered by John				
10/24/2016 11:19	Miner	$39.00		Remove
Received and entered by John				
10/24/2016 12:39	Walworth	$290.00	Approve 5.7.4	Remove

5.7.2

Save to Spreadsheet 5.7.5

County to State SCRAM Disbursement

24/7 Program

DCI - Administrator

Main Admin Search No Shows New Participant Help Logout

SCRAM Disbursements 5.8

DCI

Unreceived Disbursements 5.8.1

5.8.2

Site	Status	Posted	Date	Amount	
Beadle	Unreceived	10/24/2016 10:19	10/24/2016	$954.00	View 5.8.3
Brookings	Unreceived	10/17/2016 14:04	10/17/2016	$2,039.00	View
	Voucher for $2,039.00 turned in to Brookings County Finance Office for this payment to the SD AG Office. (John Doe)				
Codington	Unreceived	10/25/2016 08:56	10/25/2016	$2,646.00	View
	Money given to Jane for disbursement				
Deuel	Unreceived	10/26/2016 17:58	10/26/2016	$200.00	View
	given to auditor				
Grant	Unreceived	10/28/2016 12:30	10/28/2016	$90.00	View
	sent to auditor				
Hamlin	Unreceived	10/27/2016 09:42	10/27/2016	$1,243.00	View
Jackson	Unreceived	05/16/2016 10:21	05/16/2016	$180.00	View
Minnehaha	Unreceived	10/24/2016 04:46	10/24/2016	$5,796.00	View
Walworth	Unreceived	10/24/2016 13:11	10/24/2016	$329.00	View
Yankton	Unreceived	10/13/2016 14:17	10/13/2016	$2,086.00	View
	Email sent to Auditor for disbursement				
	Unreceived	09/07/2016 15:52	09/07/2016	$1,178.00	View
	Sent to Auditor for disbursement				
Total:				$16,741.00	

Undisbursed Payments 5.8.5

Site	Status	Posted	Date	Amount	
Beadle	Undisbursed			$180.00	View 5.8.6
Brookings	Undisbursed			$1,445.00	View
Brown	Undisbursed			$5,544.00	View
Butte	Undisbursed			$140.00	View
Turner	Undisbursed			$1,720.00	View
Union	Undisbursed			$3,710.00	View
Wagner PD	Undisbursed			$6.00	View
Walworth	Undisbursed			$90.00	View
Yankton	Undisbursed			$2,443.00	View
Total:				$56,621.40	

County to State Disbursement - Continued

Received Payments 5.8.7

From 10/30/2015
To 10/30/2016
update

5.8.8

Site	Status	Posted	Date	Amount	
Beadle	Received	09/26/2016 13:54	09/26/2016	$580.00	View 5.8.9
	Received	08/31/2016 14:39	08/31/2016	$760.00	View
	Received 781.00	07/25/2016 10:45	07/25/2016	$781.00	View
	Received	06/27/2016 15:10	06/27/2016	$562.00	View
	Received	05/31/2016 11:22	05/31/2016	$1,455.00	View
	Received 540.00	04/25/2016 11:07	04/25/2016	$540.00	View
Ziebach	Received	12/23/2015 11:34	12/23/2015	$120.00	View
	Received Received and entered by John.	11/09/2015 09:36	11/09/2015	$180.00	View
Total:				$1,304,457.72	

24/7 Program

DCI - Administrator Main Admin Search No Shows New Participant Help Logout

SCRAM Disbursement Details

Beadle

Disbursement

Amount $954.00
Date 10/24/2016 00:00
Status Unreceived
Comments

Change Status 5.84

Name	Posted	Date	Amount	Receipt Number
Smith, John J	09/28/2016 15:22	09/28/2016	$180.00	Receipt #44521
Smith, John Jacob	10/24/2016 09:16	10/24/2016	$180.00	Receipt #45239
Smith, Jane A	09/27/2016 09:15	09/27/2016	$60.00	Receipt #44478
Smith, Jane Ann	10/11/2016 12:17	10/11/2016	$120.00	Receipt #44911
Smith, John J	10/24/2016 10:04	10/24/2016	$150.00	Receipt #45243
Smith, John Jacob	09/27/2016 14:20	09/27/2016	$84.00	Receipt #44482
Smith, Jane A	10/22/2016 12:46	10/22/2016	$180.00	Receipt #45204
Total:			$954.00	

State to County SCRAM Disbursement

24/7 Program

DCI - Administrator | Main | Admin | Search | No Shows | New Participant | Help | Logout

5.9

Name	Balance
Armour PD	$0.00
Beadle 5.9.1	$97.00 5.9.2
Bennett	$0.00
Bon Homme	$0.00
Brookings	$695.00
Brown	$472.00
Brule	$0.00
Butte	$241.00
Charles Mix	$241.00
Clark	$0.00
Clay	$2.00
Codington	$1,203.00

24/7 Program

DCI - Administrator | Main | Admin | Search | No Shows | New Participant | Help | Logout

Site SCRAM Account

Beadle

Add a Disbursement 5.9.3

Amount

All disbursement amounts will be subtracted from the balance.

Date 10/30/2016 19:46

Comments

Add Disbursement

Add a Balance Adjustment 5.9.4

Amount

If you're adjusting the balance to subtract from it, then it has to have a – (negative) in front of the dollar amount.

Date 10/30/2016 19:46

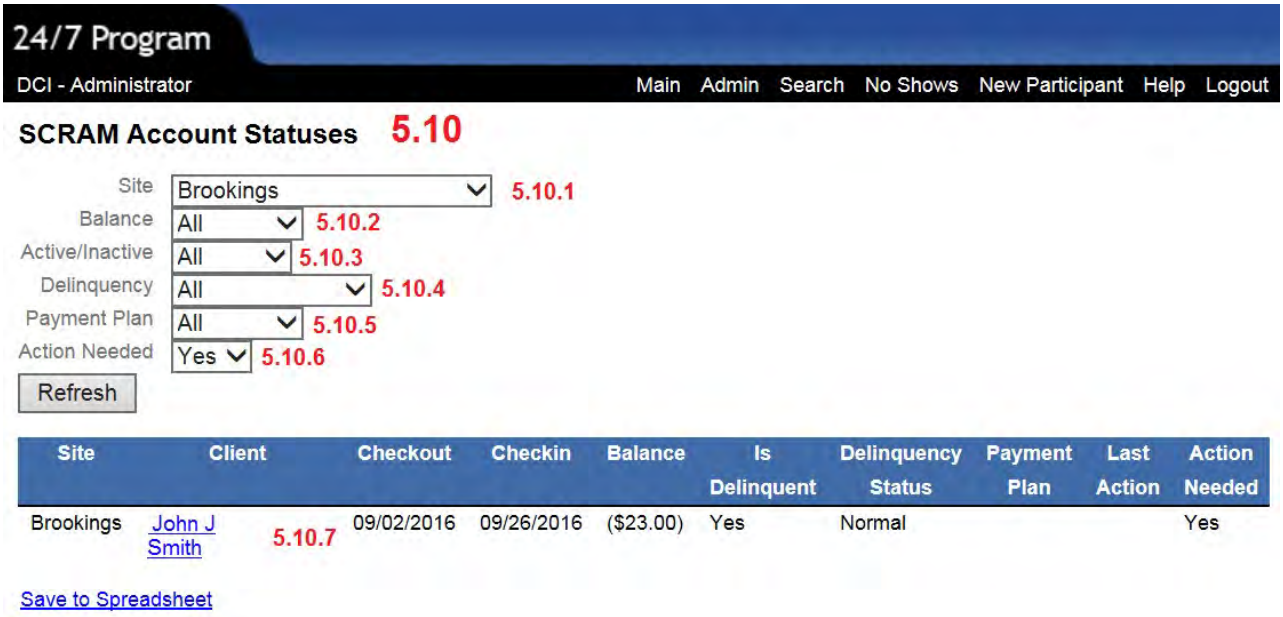
Comments

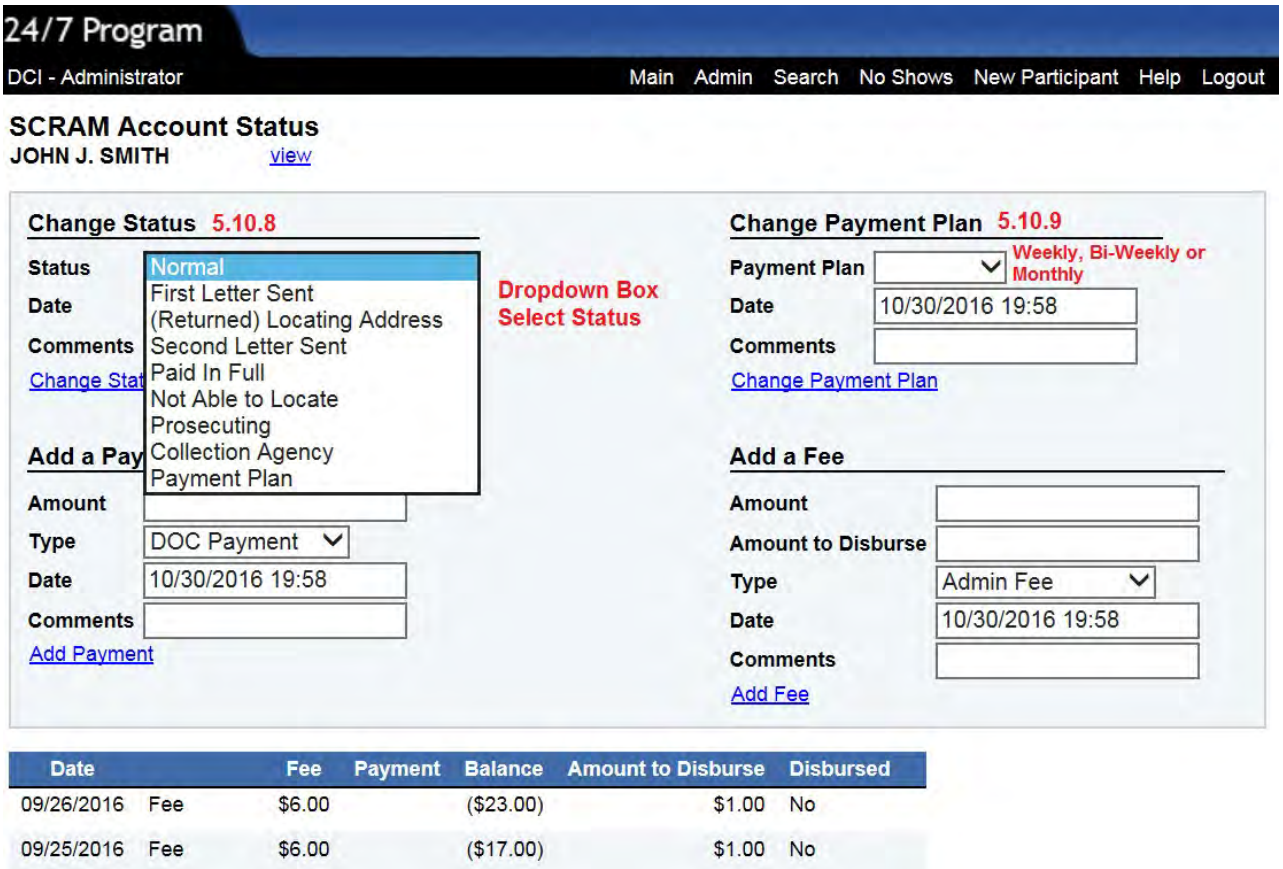
Add Adjustment

Date		Amount	Balance	
10/25/2016 01:30	Fees Accrued	$30.00	$97.00	View 5.9.6
10/23/2016 01:30	Fees Accrued	$33.00	$67.00	View
10/21/2016 01:30	Fees Accrued	$34.00	$34.00	View
10/01/2016 00:00	Disbursement	($349.00)	$0.00	
09/27/2016 01:30	Fees Accrued	$30.00	$349.00	View

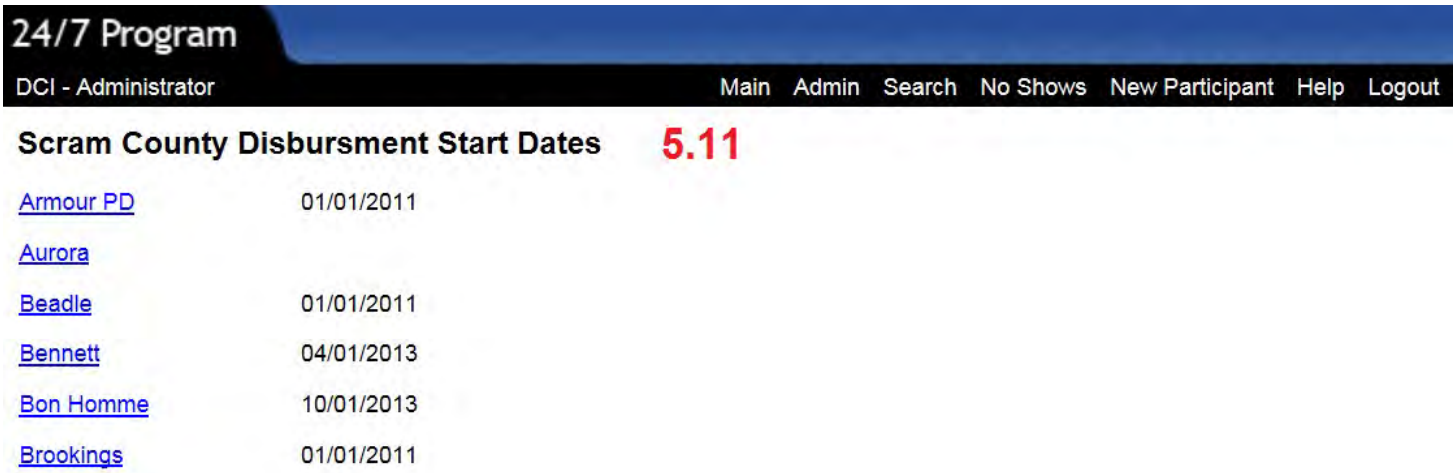
5.9.5

SCRAM Account Status

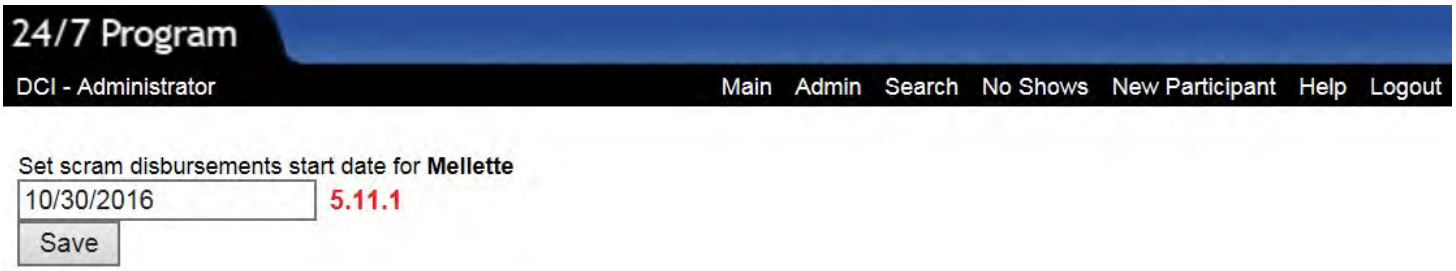




SCRAM Disbursement Start Dates



Set SCRAM Disbursements Start Date



SCRAM Fee Gaps

Participant Link

Daily Activity

24/7 Program **5.14**

DCI - Administrator

Main Admin Search No Shows New Participant Help Logout

From 10/01/2016
To 10/31/2016 5.14.1
Site DCI 5.14.2

Date	Participant	Type	Result	Testing Officer	PBT Value	Fee	Payment	Receipt#
10/25/2016 8:00	Doe, John	2x PBT	Passed	JD		$1.00		
10/25/2016 17:00	Doe, John	2x PBT	Passed	JD		$1.00		
10/26/2016 8:00	Doe, John	2x PBT	Passed	JD		$1.00		
10/26/2016 17:00	Doe, John	2x PBT	Passed	JD		$1.00		
10/27/2016 8:00	Doe, John	2x PBT	Passed	JD		$1.00		
10/27/2016 17:00	Doe, John	2x PBT	Passed	JD		$1.00		
10/28/2016 12:00	Doe, John	2x PBT	Excused			$0.00		
Jail								
10/29/2016 11:53	Doe, John	SCRAM	Activation Fee	John Doe		$40.00		
10/29/2016 11:54	Doe, John	Payment					$2.00	1152
10/29/2016 11:54	Doe, John	Payment					$10.00	1153
10/29/2016 11:55	Doe, John	Payment					$10.00	1154
10/29/2016 11:55	Doe, John	Payment					$40.00	1155
10/29/2016 11:55	Doe, John	Payment					$80.00	1156
10/29/2016 12:10	Doe, John	Payment					$40.00	1158
Initial Set Up/Inspection								
10/29/2016 12:14	Doe, John	Interlock	Activation Fee	John Doe		$40.00		

Save to Spreadsheet 5.14.3

Fees Earned

24/7 Program **5.15**

DCI - Administrator

Main Admin Search No Shows New Participant Help Logout

Fees Earned

From 9/1/2016
To 9/30/2016

5.15.1

Site	1x PBT	2x PBT	UA	Drug Patch
Armour PD	$0.00	$0.00	$0.00	$0.00
Aurora	$0.00	$0.00	$0.00	$0.00
Beadle	$28.00	$2,792.00	$1,740.00	$0.00
Bennett	$18.00	$1,158.00	$330.00	$0.00
Beresford PD	$0.00	$0.00	$0.00	$0.00
Bon Homme	$0.00	$179.00	$0.00	$0.00
Brookings	$0.00	$1,448.00	$360.00	$2,160.00
Brown	$22.00	$4,505.00	$1,010.00	$0.00
Brule	$59.00	$635.00	$210.00	$0.00
Buffalo	$0.00	$0.00	$0.00	$0.00
Butte	$67.00	$777.00	$50.00	$280.00
Charles Mix	$0.00	$723.00	$820.00	$0.00
Yankton	$4.00	$1,577.00	$2,680.00	$320.00
Ziebach	$0.00	$0.00	$0.00	$0.00

5.15.2

Save to Spreadsheet 5.15.3

Duplicate Fees and Payments

24/7 Program **5.16**

DCI - Administrator

Main Admin Search No Shows New Participant Help Logout

From 10/28/2016
To 10/31/2016

5.16.1

Refresh

Possible Duplicate SCRAM Fees 5.16.2

Date	Participant	Type	Description	Amount

Total: 0

Possible Duplicate SCRAM Payments 5.16.3

Date	Participant		Type	Description	Amount
10/28/2016	Smith, John J	HKM26DN7	SCRAM	Payment	$40.00
10/28/2016	Smith, John Jacob	HKM26DN7	SCRAM	Payment	$40.00
10/28/2016	Smith, Jane A	GX6GSD95	SCRAM	Payment	$100.00
10/28/2016	Smith, Jane Ann	GX6GSD95	SCRAM	Payment	$100.00
10/28/2016	Smith, John J	2FDKMG5R	SCRAM	Payment	$40.00
10/28/2016	Smith, John Jacob	2FDKMG5R	SCRAM	Payment	$40.00

Total: 6

5.13.4

Test Stats.

24/7 Program **5.18**

DCI - Administrator | Main | Admin | Search | No Shows | New Participant | Help | Logout

From 02/01/2007
To 10/31/2016 **5.18.1**
Site All **5.18.2**
Update

PBT Stats: **5.18.3**
02/01/2007 - 11/01/2016

41,401 participants
8,625,037 number of tests administered
8,545,709 (99.08 %) passed tests
28,176 tests failed
21114 participants were 100% Compliant
7366 failed 1 test
4679 failed 2 tests
8242 failed 3 or more tests
51,152 no show

UA Stats: **5.18.4**
07/01/2007 - 11/01/2016

7,885 participants
203,493 number of tests administered
193,846 (95.26 %) passed tests
7,603 tests failed
4619 participants were 100% Compliant
1729 failed 1 test
609 failed 2 tests
928 failed 3 or more tests
2,044 no show

Drug Patch Stats: **5.18.5**
07/01/2007 - 11/01/2016

783 participants
6,621 number of tests administered
4,376 (66.09 %) passed tests
548 tests failed
476 participants were 100% Compliant
127 failed 1 test
57 failed 2 tests
73 failed 3 or more tests

Save to Spreadsheet **5.18.6**

Action Log

24/7 Program **5.19**

DCI - Administrator | Main | Admin | Search | No Shows | New Participant | Help | Logout

Action Log

5.19.1
From 10/01/2016 To 10/31/2016

+ 10/31/2016 1:31:17 AM COMPLETED run_nightly_job **5.19.2**
10/31/2016 1:30:04 AM STARTING run_nightly_job

Records Pending Removal

+

24/7 Program **5.20**

DCI - Administrator

Main Admin Search No Shows New Participant Help Logout

Record Removal Requests

Tests

Site	Requested By	Participant	Date	Type	Result	PBT Value	Fee	Select All
Beadle	Jane Doe	John Jacob Smith	11/1/2016 9:35	2x PBT	Excused		$0.00	☐
The corresponding state fee is not automatically accounted for and requires manual removing.								
gave date of 11-1 instead of 10-31								
Beadle	Jane Doe	Jane Ann Smith	10/31/2016 8:47	2x PBT	Passed	.000	$1.00	☐
The corresponding state fee is not automatically accounted for and requires manual removing.								
entered twice								
Beadle	Jane Doe	John Smith	10/28/2016 8:43	U/A	Passed		$10.00	☐
The corresponding state fee is not automatically accounted for and requires manual removing.								
wrong								
Bennett	Jane Doe	Jane Smith	10/29/2016 20:58	2x PBT	Passed	.00	$1.00	☐
The corresponding state fee is not automatically accounted for and requires manual removing.								
accidently got logged twice eric kiefer 11-1k								

REMOVE DENY

Drug Patches

Type	Site	Removed By	Participant	Date	Fee	Select All
Patch Application	Brookings	Jane Doe	John Jacob Smith	10/31/2016 9:28	$40.00	☐
Applied At: 11/11/2016 18:00, Removal Scheduled: 10/31/2016 09:28						
WRONG PATCH NUMBER						

REMOVE

Payments

Site	Requested By	Participant	Date	Amount	Select All
Fall River	Jane Doe	John Jacob Smith	10/30/2016 6:07	$1.00	☐
wrong amount					
Fall River	Jane Doe	Jane Ann Smith	10/30/2016 7:15	$4.00	☐
wrong date of actual payment					
Pennington	Jane Doe	John Smith	10/29/2016 18:17	$10.00	☐
only 10					

REMOVE DENY

Users

Name	Username	Requested By	Select All

REMOVE DENY

APPENDIX B –Contract Terms and Conditions (Include Exhibit C)

STATE OF SOUTH DAKOTA

CONSULTING CONTRACT

Agreement made and entered into this_____day of_____,_____,

by and between

South Dakota Office of the Attorney General, a state agency, of

(Name of Agency)

1302 E. Highway 14 , Pierre , SD , 57501 , (the "State")

(Address) (City) (State) (Zip Code)

and_____,_____,

(Company Name) (Address)

_____,_____,_____,

(City) (State) (Zip Code)

_____ (the "Vendor").

(Phone Number)

The State hereby enters into this Agreement for services with Vendor in consideration of and pursuant to the terms and conditions set forth herein.

The terms of the attached Work Plan, attached hereto as Exhibit A; Appendix, attached hereto as Exhibit B; and Confidentiality Provision, attached hereto as Exhibit C, are incorporated into this Agreement as if fully set forth herein.

1. The Vendor will perform those services described in the Work Plan, attached hereto as Exhibit A.

2. The Vendor's services under this Agreement shall commence on _____ and end on_____, unless sooner terminated pursuant to the terms hereof.

3. The Vendor will not use State equipment, supplies or facilities. The Vendor will have access to all servers, software and applications of the State system necessary for the installation, configuration, modification and maintenance of _____. The State shall cooperate with Vendor and provide Vendor with such assistance as Vendor may reasonably require under this Agreement. The Vendor will provide the State with its Employer Identification Number, Federal Tax Identification Number or Social Security Number upon execution of this Agreement.

4. The State will make payment for services upon satisfactory completion of the services. The TOTAL CONTRACT AMOUNT is an amount not to exceed $_____. The State will not pay Vendor's expenses as a separate item. Payment will be made by the State within forty-five (45) days of the date of an itemized invoice submitted by Vendor with a signed state voucher.

Payment will be made consistent with SDCL ch. 5-26. The Vendor acknowledges that it would be difficult or impracticable for the State to provide the notice of disagreement provided for by SDCL 5-26-5 within the ten days provided for by that section. Accordingly, Vendor hereby agrees that the State shall have thirty (30) days to provide the requisite notice of disagreement.

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

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

A. Commercial General Liability Insurance:

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

B. Professional Liability Insurance or Miscellaneous Professional Liability Insurance:

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

C. Business Automobile Liability Insurance:

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

D. Worker's Compensation Insurance:

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

Before beginning work under this Agreement, Vendor shall furnish the State with properly executed Certificates of Insurance which shall 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 Vendor agrees to provide immediate notice to the State and provide a new certificate of insurance showing continuous coverage in the amounts required. Vendor shall furnish copies of insurance policies if requested by the State.

7. While performing services hereunder, the Vendor is an independent vendor and not an officer, agent, or employee of the State of South Dakota.

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

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

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

Upon notice of termination, by either party, the State will be provided by the Vendor all current state proprietary information, state data, and end user data in a non-proprietary form. Upon the effective date of the termination of the Agreement the State will again be provided by the Vendor with all current state proprietary information, state data and end user data in a non-proprietary form.

In the event of termination, the Vendor shall deliver to the State all reports, plans, specifications, technical data, and all other information completed prior to the date of termination.

In the event that the Vendor fails to complete the project or any phase thereof within the time specified in the Work Plan, attached as Exhibit A, or within such additional time as may be granted in writing by the State, or fails to prosecute the work, or any separable part thereof, with such diligence as will insure its completion within the time specified in the Work Plan or any extensions thereof, the State shall be authorized to terminate the Agreement for default and suspend the payments scheduled as set forth elsewhere in this Agreement.

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, this Agreement will be terminated by the State. Termination for any of these reasons is not a default by the State nor does it give rise to a claim against the State.

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 shall be expressly identified as a part hereof, and be signed by an authorized representative of each of the parties hereto.

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

13. The Vendor 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.

14. The Vendor may not use subcontractors to perform the services described herein without the express prior written consent of the State. The Vendor 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 Vendor will cause its subcontractors, agents, and employees to comply, with applicable federal, state and local laws, regulations, ordinances, guidelines, permits and requirements and will adopt such review and inspection procedures as are necessary to assure such compliance.

The State, at its option, may require the vetting of any subcontractors and or agents. The Vendor is required to assist in this process as needed. The State reserves the right to reject any person from the project who the State believes would be detrimental to the project or is considered by the State to be a security risk.

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

15. The Vendor certifies that neither Vendor 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. Vendor further agrees that it will immediately notify the State if during the term of this Agreement Vendor 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.

16. Any notice or other communication required under this Agreement shall be in writing and sent to the address set forth above. Notices shall be given by and to _____ on behalf of the State, and by_____, on behalf of the Vendor, or such authorized designees as either party may from time to time designate in writing. Notices or communications to or between the parties shall be

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

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

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 herein, this Agreement constitutes the entire agreement with respect to the subject matter hereof.

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

20. The State of South Dakota requires all employee(s) of the Vendor, subcontractor(s) and or agent(s) 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 have access to secure areas to have finger-print 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 the procedure that is to be used to process the finger print cards. If work assignments change after the initiation of the project covered by this agreement so that employee(s) of the Vendor, subcontractor(s) and or agent(s) 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 have access to secure areas then finger-print based background checks must be performed on any employees who will complete any of the referenced tasks. The State reserves the right to require the Vendor to prohibit any employee, subcontractor or agent 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 Vendor with notice of its determination.

21. The confidentiality provision (attached hereto as Exhibit C), liability and indemnification provisions of this Agreement are intended to survive termination of this Agreement.

22. Notwithstanding anything in this Agreement to the contrary, neither party shall be liable for any delay or failure to perform under the terms and conditions of this Agreement, if the delay or failure is caused by war, terrorist attacks, riots, civil commotion, fire, flood, earthquake or any act of God, or other causes beyond the party's reasonable control. Provided, however, that in order to be excused from delay or failure to perform, the party must act diligently to remedy the cause of such delay or failure and must give notice to the other party as provided in this Agreement as soon as reasonably possible to explain the length and cause of the delay in performance.

23. Vendor 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. 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. This paragraph shall control and supersede the language of any such agreements to the contrary.

24. Pursuant to South Dakota Codified Law 1-33-44, the Bureau of Information and Telecommunications ("BIT") oversees the acquisition of office systems technology, software and services; telecommunication equipment, software and services; and data processing equipment, software, and services for departments, agencies, commissions, institutions and other units of state government. BIT requires the contract provisions which are attached to this Agreement as Exhibit B – Appendix and incorporated into this Agreement by reference. It is understood and agreed to by all parties that BIT, as the State's technology governing organization, has reviewed only Exhibit B – Appendix of this agreement.

In Witness Whereof, the parties signify their agreement effective the date below first written by the signatures affixed below. By signing this agreement, the Bureau of Information and Telecommunications (BIT) is representing that as the State's technology governing organization it has reviewed only the technical provisions of this agreement.

State	**Vendor**
_____	_____
(Signature)	(Signature)
BY: Marty Jackley _____	BY: _____
(Name)	(Name)
Attorney General _____	_____
(Title)	(Title)
South Dakota Office of the Attorney General	_____
(State Agency)	(Vendor)
_____	_____
(Date)	(Date)

BY: _____
(David Zolnowsky)

Bureau of Information and Telecommunications
(Commissioner)

_____
(Date)

-Name and phone number of contact person in State Agency who can provide additional information regarding this contract, please contact Kay McLain at 605-773-3215.
-This contract will be paid out of the following funds:

EXHIBIT A
WORK PLAN

EXHIBIT B
APPENDIX

EXHIBIT C
CONFIDENTIALITY PROVISION

1. In order for Vendor to perform the computer programming services contemplated under the Agreement, Vendor may require access to confidential information.
2. Vendor acknowledges the State's need to keep confidential information it maintains, that is subject to various confidentiality statutes and legal privileges held by the State as well as other agencies, state agency clients, in-state and out-of-state government entities, and third parties.
3. Vendor agrees that in order to protect the confidentiality and legal privileges associated with State computer usage and data storage that it and all of its officers, agents, and employees:
    a. Will not, at any time, either directly or indirectly, make public, reveal, or communicate to any person, firm, or corporation or public entity, in any manner whatsoever, any information concerning any matters affecting or relating to confidential records or data that may be obtained in the course of performing this Agreement.
    b. Will not reproduce or transfer in any way or manner or share with any person, except as specifically authorized by the State, any confidential data or information provided by the State.
    c. Will not read, review, monitor, access, or attempt entry or other accession, of any data, documents, records, files (private or public), databases, communications, research trails, cookies, hard drives, servers, back up tapes or other back up mechanisms or facilities, on any State computer.
4. If work assignments performed in the course of this Agreement require additional security requirements or clearance, the Vendor agrees that its officers, agents and employees may be required to undergo investigation or may be required to sign separate confidentiality agreements, and it will limit access to the confidential information and related work activities to employees that have executed such agreements.
5. Vendor will enforce the terms of this Confidentiality Provision to its fullest extent. Vendor agrees to prohibit any employee or agent from performing work under this Agreement that has or is suspected to have violated the terms of this Confidentiality Provision.
6. Violation of this Confidentiality Provision is cause for immediate termination of this Agreement and could subject any violator to criminal prosecution in accordance with state law.

7. Neither this Confidentiality Provision, nor any part thereof, shall establish any privacy rights to, for, or on the part of, any employee of the Vendor or State or waive any remedies against any such person for illegal, improper, or unauthorized use of the computers or any computer system or portion thereof.
8. Vendor understands that the State is subject to certain obligations regarding public information under South Dakota's open records laws, which include SDCL ch. 1-27.

APPENDIX C – Included I/T Contract Terms and Conditions– Vendor Hosted Proposal
Contract Exhibit B

1. The Vendor will perform those services described in the Work Plan, attached hereto as Exhibit A.

a. In the performance of these services and providing the deliverables under the Agreement, Vendor, and its employees shall exercise the degree of skill and care consistent with customarily accepted practices and procedures for the performance of the type of services required. The Vendor shall be responsible for the professional quality, technical accuracy, timely completion, and coordination of all services and deliverables furnished by the Vendor and any subcontractors, if applicable, under this Agreement.

b. Vendor represents and warrants that:

i. It shall give high priority to the performance of the services; and

ii. The services shall be performed in a timely manner.

c. It shall be the duty of the Vendor to assure that its services and deliverables are technically sound and in conformance with all pertinent technical codes and standards.

d. The Vendor shall be responsible to the State for material deficiencies in the contracted deliverables and services which result from the failure to meet the standard given herein. Vendor shall promptly correct or revise any material errors or omissions in deliverables and re-perform any services which are not in compliance with such representations and warranties at no cost to the State, provided that Vendor's failure to comply is not related or attributable, in whole or in part, to the actions, errors or omissions of the State.

e. Permitted or required approval by the State of any services or deliverables furnished by the Vendor shall not in any way relieve the Vendor of its responsibility for the professional quality and technical accuracy and adequacy of its work. The State's review, approval, acceptance, or payment for any of the Vendor's services or deliverables herein shall not be construed to operate as a waiver of any rights under this Agreement or of any cause of action arising out of the performance of this Agreement, and except as provided herein the Vendor shall be and remain liable in accordance with the terms of this Agreement and applicable law for all damages to the State caused by the Vendor's performance or failure to perform under this Agreement.

f. In the event of a breach of these representations and warranties, Vendor shall immediately, after telephonic notice from the State, begin work on curing such breaches. If it is necessary for Vendor to send at least one qualified and knowledgeable representative to the State's site where the system is located, this will be done at Vendor's sole expense. 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. In connection with the performance of this Agreement and the provision of services and

deliverables under this Agreement, neither party will infringe any patent, copyright, trademark, trade secret or other proprietary right of any person. Neither party will improperly use any trade secrets or confidential or proprietary information owned by any third party in performing this Agreement or the services related to this Agreement.

3. The Vendor represents and warrants that it has the full power and authority to grant the rights described in this Agreement without violating any rights of any third party, and that there is currently no actual or, to Vendor's knowledge, threatened suit by any such third party based on an alleged violation of such rights by Vendor. The Vendor further represents and warrants that the person executing this Agreement for Vendor has actual authority to bind Vendor to each and every term, condition and obligation to this Agreement, and that all requirements of Vendor have been fulfilled to provide such actual authority.

4. In accordance with Section 5 of this Agreement, Vendor will, at its expense, indemnify, defend and hold harmless State and its affiliates, and their respective successors and assigns, and their respective directors, officers and employees, from and against any and all claims, demands, suits, action and any and all damages, losses, liabilities, taxes, penalties, fines, charges, costs and expenses (including reasonable attorneys' fees) arising from or relating to a third party claim that any of the services or deliverables provided by Vendor to the State under this Agreement infringes that party's U.S. patent, U.S. trademark or copyright or misappropriates that party's trade secret or other intellectual property right, provided, however, Vendor shall not be required to indemnify State and its affiliates for any claims that result from or are related to: (i) the State's or other party's combination, operation, or use of the software in a manner not specifically authorized by Vendor; or (ii) alterations or modifications to the software not performed or authorized by Vendor.

If such a third party claim is made or appears likely to be made, Vendor, in its sole discretion, may elect: (i) to procure for State the right to continue to use the software product; (ii) to replace, at Vendor's cost, the software product, or any portion thereof, with a substitute product that functions substantially in accordance with the product's specifications; (iii) to modify the software product so that it does not infringe or misappropriate, provided that the product, as modified, continues to perform substantially in accordance with the applicable specifications.

Vendor's obligation to indemnify the State hereunder will be contingent on the State (i) notifying the Vendor in writing of the claim; (ii) allowing the Vendor the ability to control, and cooperating with Vendor in, the defense thereof and any related settlement negotiations; and (iii) in no event, agreeing to, or authorizing settlement of, any such claim without Vendor's prior written agreement, which such consent shall not be unreasonably withheld, conditioned or delayed. Vendor will reimburse State's reasonable out-of-pocket expenses incurred in providing assistance regarding any claim.

5. Vendor further represents and warrants that:

a. Vendor is an organization duly organized, validly existing and in good standing under the laws of its state of organization and has all requisite corporate power and authority to execute, deliver and perform its obligations under this Agreement;

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

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

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

e. Vendor's methods of accounting are consistent with Generally Accepted Accounting Principles (GAAP) and are capable of segregating costs by stage, segment, or cost objective in order to support change order accounting.

6. 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/ .

7. SECURE PRODUCT DEVELOPMENT: Consistent with the provisions of the agreement, the Vendor, subcontractor and or agent shall use the highest applicable industry standards for sound secure software development practices to resolve critical security issues as quickly as possible. These standards include but are not limited to the South Dakota Application Security Vulnerabilities document found at http://cybersecurity.sd.gov/docs/development/DevelopmentSecurityItems.pdf. Items listed under Section A of the South Dakota Security Vulnerabilities document may not be present in the software. Continued compliance to these standards is required as the standards will change over time. The "highest applicable industry standards" shall also be defined as the degree of care, skill, efficiency, and diligence that a prudent person possessing technical expertise in the subject area and acting in a like capacity would exercise in similar circumstances.

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

A. Name of the person responsible for certifying that all deliverables are secure.

B. Documentation detailing the vendor's version upgrading process (for those applications where there is or will be a maintenance agreement).

C. Notification of application patches and updates (for those applications where there is/will be a maintenance agreement).

D. List of tools used in the software development environment used to verify secure coding.

E. Based on a risk assessment, provide the State the secure configuration guidelines, specifications and requirements that describe security relevant configuration options and their implications for the overall security of the software. The guidelines, specifications and requirements must include descriptions of dependencies on the supporting platform, including operating system, web server, application server and how they should be configured for security. The default configuration of the software shall be secure.

At the State's discretion the State will discuss the security controls used by the State with the

Vendor upon the Vendor signing a non-disclosure agreement.

8. THREAT NOTIFICATION: Upon becoming aware of a possible security threat(s) or exploit(s) with the Vendor's product(s) and or service(s) being used by the State the Vendor will notify the State within two (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).

9. SECURITY INCIDENT AND BREACH NOTIFICATION:

A. The Vendor, unless stipulated otherwise, shall notify the State Contact within 12 hours if the Vendor 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.

B. Notification to the State should include at a minimum all data available including: (i) Name of and contact information for the Vendor's Point of Contact for the security incident or data breach: (ii) date and time of the security incident or data breach; (iii) date and time the security incident or data breach was discovered: (iv) description of the security incident or data breach including the data involved, being as specific as possible; (v) potential number of records known, and if unknown the range of records; (vi) address where the security incident or data breach occurred: and, (vii) the nature of the technologies involved. Notifications must be sent electronically and encrypted via NIST or other applicable federally approved encryption techniques. If there are none use AES-256 encryption with SHA-256 or SHA-2 hashing. Vendor shall use the term "data incident report" in the subject line of the email. If not all of the information is available for the notification within the specified time period Vendor shall provide the State with all of the available information.

10. HANDLING OF DATA BREACHES: If applicable, the Vendor 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 Vendor 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 Vendor will use a credit monitoring service, forensics company, advisors and public relations firm that are acceptable to the State, 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 Vendor shall inform the State of actions being taken or will be taken to reduce the risk of further loss to the State.

Except as otherwise required by law, the Vendor shall only provide notice of the incident to the State. The State will determine whether notification to the affected parties will (i) jeopardize the State's interests and (ii) be more appropriate for the Vendor to make. The method and content of the notification of the affected parties must be coordinated with, and is subject to, approval by the State. If the Vendor is required by federal law or regulation to conduct a security incident or data

breach investigation, the results of the investigation must be reported to the State. If the Vendor is required by federal law or regulation to notify the affected parties, the State must also be notified.

Notwithstanding any other provision of this agreement, and in addition to any other remedies available to the State under law or equity, the Vendor will reimburse the State in full for all costs incurred by the State in investigation and remediation of the data breach including, but not limited, to providing notification to third parties whose data were compromised and to regulatory agencies or other entities as required by law or contract. The Vendor shall also reimburse the State in full for all costs the State incurs in its offering of 3 years credit monitoring to each person whose data were compromised. The Vendor shall also pay any and all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the data breach.

11. BROWSER: 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.

12. THIRD PARTY HOSTING: If the Vendor has the State's and End User's data, which is data___, hosted by another party the Vendor must provide the State the name of this party The Vendor must provide the State with contact information for this third party and the location of their data center(s). The Vendor must receive from the third party written assurances that the State and End User data will reside in the continental United States at all times and provide these written assurances to the State. If during the term of this agreement the vendor changes from the Vendor hosting the data to a third-party hosting the data or changes third-party hosting provider, the Vendor will provide the State with one hundred and eighty (180) days' advance notice of this change and at that time provide the State with the information required above.

13. SOURCE CODE ESCROW:

A. Deposit in Escrow: "Source Code" means all source code of the Software, together with all commentary and other materials supporting, incorporated into or necessary for the use of such source code, including all supporting configuration, documentation, and other resource files and identification by Vendor and version number of any software (but not a license to such third-party software) used in connection with the source code and of any compiler, assembler, or utility used in generating object code.

   Within ninety (90) days of the effective date, Vendor shall deposit the Source Code for the software with a nationally recognized software escrow company (subject to the approval of the State, not to be unreasonably withheld) (the "Escrow Agreement"). Within thirty (30) days after delivery to the State of any major update, Vendor shall deposit the Source Code for such update with the Escrow Agent pursuant to the Escrow Agreement. For all other updates, Vendor shall deposit the Source Code for such updates on a semiannual basis with the Escrow Agent pursuant to the Escrow Agreement.

   The parties agree that the Escrow Agreement is an "agreement supplementary to" the Agreement as provided in Section 365(d) of Title 11, United States Code (the "Bankruptcy Code"). Immediately upon termination of this Agreement, the Source Code shall be released back to Vendor.

B. Conditions for release: The State will have the right to obtain the Source Code in accordance with and subject to the terms and conditions of this Section and the Escrow Agreement provided that all of the following three conditions are met (collectively a "Release Event"):

1. Vendor winds down its business or liquidates its business under a Chapter 7 Bankruptcy proceeding; or Vendor discontinues maintenance and support to the Software,

2. No entity has succeeded to Vendor's obligations to provide maintenance and support on the Software in accordance with the Agreement in effect between the parties, and

3. The State is not in breach of its obligations under this Agreement.

C. Source Code: In no event shall the State have the right to use the Source Code "barring a release event" for any purpose, and the State is specifically prohibited from using the Source Code to reverse engineer, develop derivative works or to sublicense the right to use the Source Code to any other person or entity for any purpose. Customer will also be obligated to treat the Source Code as Confidential Information of Vendor under the Agreement.

D. The cost for establishing and maintaining the Escrow Account will be that of the State.

14. DISASTER RECOVERY:

The Vendor will maintain a disaster recovery plan (the "Disaster Recovery Plan") with respect to the services provided to the State. For purposes of this Agreement, a "Disaster" shall mean any unplanned interruption of the operation of or inaccessibility to the Vendor's service in which the State, using reasonable judgment, requires relocation of processing to a recovery location. The State shall notify the Vendor as soon as possible after the State deems a service outage to be a Disaster. The Vendor shall move the processing of the State's services to a recovery location as expeditiously as possible and shall coordinate the cut-over.

15. AUDIT: When hosting any state data that may be confidential, private, financially sensitive, or contain personally identifiable information, the vendor must agree to:

Allow State, at Vendor's expense, twice annually, a security audit and vulnerability assessment to provide third party verification of Vendor's IT security safeguards for the system and its data and/or that of the company and its policies and procedures. At its request, the State may review any and all independent audit reports that document the system's and company's policies and/or procedure's security posture. This security audit and vulnerability assessment must come from a third party source agreed to in advance by the State.

The Vendor agrees to work with the State to rectify any serious security issues revealed by the security audit and vulnerability assessments. This includes additional security audits and vulnerability assessments that shall be performed after any remediation efforts to confirm the security issues have been resolved and no further security issues exist. It is required that any security audits must meet the requirements of the Payment Card Industry Data Security Standard (PCI DSS) irrespective of there being any PCI DSS data involved.

16. FACILITIES INSPECTION: The Vendor grants authorized state and/or federal personnel access to inspect their systems, facilities, work areas, contractual relationships with third parties involved in supporting any aspects of the Vendor hosted system, and the systems which support/protect the Vendor hosted system. This access will be granted on 24 hour notice. Such personnel will be limited to staff authorized by the State or the federal government to audit the system, and representatives of the State entity that funds the hosting. The State accepts that access will be arranged with an escort, and the Vendor commits that the escort will have the access and authority to provide physical access to facilities, answer appropriate questions, and provide requested documentation, including but not limited to executed contract terms, operating procedures, records of drills and tests, evidence of background checks, security logs, and any other items required by state or federal audit requirements or as deemed by the State to be required to demonstrate the Vendor is complying with all contract terms.

17. REDUNDANT POWER AND COOLING TO ALL HARDWARE: The Vendor will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate all facilities supporting the application have adequate redundant power and cooling capacity to operate uninterrupted, and without the need to refuel generators, for not less than 24 hours in the event the local external power fails.

18. UPS BACKUP: The Vendor will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate that all facilities supporting the application have adequate UPS power to carry the systems for not less than 10 minutes, and to protect the system from power fluctuations including, but not limited to, surge, spikes, sags, and instability.

19. RIGHTS AND LICENSE IN AND TO STATE AND END USER DATA: The parties agree that between them, all rights including all intellectual property rights in and to State and End User data shall remain the exclusive property of the State, and that the Vendor has a limited, nonexclusive license to use these data as provided in this Agreement solely for the purpose of performing its obligations hereunder. This Agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the Agreement.

20. MIGRATION CAPABILITY: Upon termination or expiration of this Agreement, the Vendor will ensure that all State and End User Data is transferred to the State or a third party designated by the State securely, within a reasonable period of time, and without significant interruption in service, all as further specified in the Technical Specifications provided in the RFP. The Vendor will ensure that such migration uses facilities and methods that are compatible with the relevant systems of the transferee, and to the extent technologically feasible, that the State will have reasonable access to State and End User Data during the transition.

The Vendor will notify the State of impending cessation of its business or that of a tiered provider and any contingency plans in the event of notice of such an event. This includes immediate transfer of any previously escrowed assets and data and State access to the Vendor's facilities to remove or destroy any State-owned assets and data. The Vendor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the State. The Vendor will provide a fully documented service description and perform and document a gap analysis by examining any differences between its services and those to be provided by its successor. The Vendor will also provide a full inventory and configuration of servers, routers, other

hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the State. The Vendor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and impact on the State, all such work to be coordinated and performed in advance of the formal, final transition date.

21. HOST FACILITY PHYSICAL SECURITY: The Vendor will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate that all facilities supporting the application have adequate physical security. This includes, at a minimum, centrally administered electronic locks that control entry and exit from all rooms where the Vendor hosted system resides. Any door security system must either be connected to the building's power backup system as defined elsewhere or have internal battery power sufficient to last 24 hours in normal usage. Security events for the physical access system must be logged and the logs stored electronically in a secure location in a non-changeable format and must be searchable. Retention on the logs must be not less than 7 years. Log entries must be created for at least: successful entry and exit (indicating whether the access was to enter or exit the room) as well as all security related events such as, doors left open more than 30 seconds, forced entries, failed entry attempts, repeat entries without exit, repeat exits without entry, attempts to access doors for which access was not authorized. The Vendor agrees to provide, at the State's request, full access to search the security logs for any access or security events related to any and all rooms and physical locations hosting the State's system.

22. SCANNING AUTHORIZATION:

The definitions immediately below apply to the following term on security scanning.

- Test Data- data that mimics the data used by the Vendor for performing the work referenced in this agreement
- Test System- infrastructure and software that duplicates the Vendor system used for performing the work referenced in this agreement, this test system will utilize test data
- Security Scanning – the utilization of software tools to interrogate the application or hardware to assess compliance with standard best practices to preserve cyber security.
- Reverse Engineering – an action used to discover the content of application code.
- Application Code – the instruction utilized by a computer application to cause the computer to perform an instruction
- Computer system- the network of computers, the supporting and peripheral devices and software used by the Vendor to perform the work referenced in this agreement

The Vendor will provide the State, at a date, time and for duration agreeable to both parties, access to a test system containing tests data for Security Scanning activities. The system and data provided to the State by Vendor for testing purposes will be considered a test system containing test data. The State will not scan any environment known by the State to be a production environment at the time the scan is performed by the State. Vendor provides their consent for the State or any third-party acting for the State to scan the systems and data provided as the State wishes using any methodology that the State wishes. Any scanning performed by the State will not be considered a violation of any licensure agreements the State has with the Vendor or that the Vendor has with a third-party. The Vendor indemnifies the State for ordinary, consequential and incidental damages to the Vendor's computer system and the data it contains that is the result of scanning. Scanning by the State or any third-party acting for the State will not be considered reverse engineering. If the State's security scans discover security issues the State may collaborate with, at the State discretion, the Vendor on remediation efforts. These remediation efforts will not be considered a violation of any licensure agreements between the State and Vendor. The State while engaged, and

after, with the Vendor on remediation is indemnified and held harmless from all actions, lawsuits, damages (including all ordinary, consequential and incidental damages) or other proceedings that arise from security scanning, remediation efforts, or any after effects of security scanning or remediation. This indemnification includes all defense costs as well as reasonable attorneys' fees the State of South Dakota is required to pay in any such proceedings. The State will not be charged for any costs incurred by the Vendor in these remediation efforts unless agreed to by the State in advance in writing. In the event of conflicting language this clause is to supersede any other language in this or any other agreement made between the State and the Vendor.

23. HOST NETWORK SECURITY: The Vendor will use industry standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing Services under this Agreement as indicated in the Information Technology User Security Guide.

The Vendor will, at its expense, either conduct or have conducted at least on an annual basis and provide to the State upon its request:

A. A vulnerability scan, performed by a scanner approved by the State, of the Vendor's systems and facilities that are used in any way to deliver services under this Agreement; and

B. A formal penetration test, performed by a process and qualified personnel approved by the State, of the Vendor's systems and facilities that are used in any way to deliver services under this Agreement.

24. LEGAL REQUESTS FOR DATA: Except as otherwise expressly prohibited by law, the Vendor will:

A. Immediately notify the State of any subpoenas, warrants, or other legal orders, demands or requests received by the Vendor seeking State and/or End User Data maintained by the Vendor;

B. Consult with the State regarding its response;

C. Cooperate with the State's requests in connection with efforts by the State to intervene and quash or modify the legal order, demand or request; and

D. Upon the State's request, provide the State with a copy of both the demand or request and its proposed or actual response.

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

26. DATA PRIVACY:

A. The Vendor will use State Data and End User Data only for the purpose of fulfilling its duties under this Agreement and for the State's and its End User's sole benefit, and will not share such data with, or disclose it to, any third party, without the prior written consent of the State or as otherwise required by law. By way of illustration and not of limitation, the Vendor will not use such data for the Vendor's own benefit and, in particular, will not engage in "data mining" of State or End User Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by the State through a State employee or officer specifically authorized to grant such use of State data

B. All State and End User Data will be stored on servers located solely within the continental United States.

C. The Vendor will provide access to State and End User Data only to those Vendor employees and subcontractors who need to access the data to fulfill the Vendor's obligations under this Agreement.

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

28. DATA RETENTION AND DISPOSAL:

A. The Vendor will use commercially reasonable efforts to retain data in an End User's account until the End User deletes them, or for an alternate time period mutually agreed by the parties.

B. Using appropriate and reliable storage media, the Vendor will regularly back up State and End User Data and retain such backup copies for a minimum of thirty-six months. At the end of that time period and at the State's election, the Vendor will either securely destroy or transmit to the State repository the backup copies. Upon the State's request, the Vendor will supply the State with a certificate indicating the nature of the storage media destroyed, the date destroyed, and the method of destruction used.

C. The Vendor will retain logs associated with End User activity for a minimum of seven years, unless the parties mutually agree to a different period.

D. The Vendor will immediately place a "hold" on the destruction under its usual storage media retention policies of storage media that include State and End User Data, in response to an oral or written request from authorized State personnel indicating that those records may be relevant to litigation that the State reasonably anticipates. Oral requests by the State for a hold on storage media destruction will be reproduced in writing and supplied to the Vendor for its records as soon as reasonably practicable under the circumstances. The State will promptly coordinate with the Vendor regarding the preservation and disposition of storage media. The Vendor shall continue to preserve the storage media until further notice by the State. The Vendor will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate that all facilities supporting the methods of disposal of storage media, are appropriate to and fulfill all of the State's needs. By way of example but not of limitation, all hard drives and tapes used to store State data must, upon destruction be properly disposed of.

29. MULTI-TENANT ARCHITECTURE LOGICALLY/PHYSICALLY SEPARATED TO INSURE DATA SECURITY: The Vendor will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate that all facilities supporting the application have adequate safeguards to assure that needed logical and physical separation is in place and enforced to insure data security, physical security, and transport security.

30. ACCESS ATTEMPTS: All access attempts, whether failed or successful, to any system connected to the Vendor hosted system which can access, read, alter, intercept, or otherwise impact

the Vendor hosted system or its data or data integrity shall be logged by the Vendor. For all systems, the log must include at least: log-in page used, username used, time and date stamp, incoming IP for each authentication attempt, and the authentication status, whether successful or not. Logs must be maintained not less than 7 years in a searchable database in an electronic format that is un-modifiable. At the request of the State, access must be granted to search those logs as needed to demonstrate compliance with the terms of this contract, and any and all audit requirements related to the Vendor hosted system.

31. PASSWORD POLICIES: Password policies for all Vendor employees will be documented annually and provided to the State to assure adequate password protections are in place. Logs and administrative settings will be provided to the State on request to demonstrate such policies are actively enforced.

32. SYSTEM UPGRADES: Advance notice of___(to be determined at contract time) shall be given to the State of any major upgrades or system changes that the Vendor will be implementing. A major upgrade is a replacement of hardware, software or firmware with a newer or better version, in order to bring the system up to date or to improve its characteristics. The State reserves the right to postpone these changes.

33. SEPARATION OF JOB DUTIES: The Vendor shall require commercially reasonable non-disclosure agreements, and limit staff access to State data to that which is required to perform job duties.

34. PROVISION OF SERVICES: The Vendor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided.

35. IDENTIFICATION OF BUSINESS PARTNERS: The Vendor shall identify all of its business partners and subcontractors related to services provided. under this contract, who will be involved in any application development and/or operations.

36. REMOVAL OF VENDOR REPRESENTATIVE: The State shall have the right at any time to require that the Vendor remove from the project any staff or subcontractor who the State believes is detrimental to the project. The State will provide the Vendor with notice of its determination, and the reasons it requests the removal. If the State signifies that a potential security violation exists with respect to the request, the Vendor shall immediately remove such individual.

37. LOCATION OF STATE AND END USER DATA: All State data hosted by the vendor will be stored in facilities located in the United States of America. At no time is it acceptable for any State data to be stored in facilities outside the United States of America. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the United States of America.

APPENDIX D – Included I/T Contract Terms and Conditions – State Hosted Proposal
Contract Exhibit B

1. The Vendor will perform those services described in the Work Plan, attached hereto as Exhibit A.

a. In the performance of these services and providing the deliverables under the Agreement, Vendor, and its employees shall exercise the degree of skill and care consistent with customarily accepted practices and procedures for the performance of the type of services required. The Vendor shall be responsible for the professional quality, technical accuracy, timely completion, and coordination of all services and deliverables furnished by the Vendor and any subcontractors, if applicable, under this Agreement.

b. Vendor represents and warrants that:

i. It shall give high priority to the performance of the services; and

ii. The services shall be performed in a timely manner.

c. It shall be the duty of the Vendor to assure that its services and deliverables are technically sound and in conformance with all pertinent technical codes and standards.

d. The Vendor shall be responsible to the State for material deficiencies in the contracted deliverables and services which result from the failure to meet the standard given herein. Vendor shall promptly correct or revise any material errors or omissions in deliverables and re-perform any services which are not in compliance with such representations and warranties at no cost to the State, provided that Vendor's failure to comply is not related or attributable, in whole or in part, to the actions, errors or omissions of the State.

e. Permitted or required approval by the State of any services or deliverables furnished by the Vendor shall not in any way relieve the Vendor of its responsibility for the professional quality and technical accuracy and adequacy of its work. The State's review, approval, acceptance, or payment for any of the Vendor's services or deliverables herein shall not be construed to operate as a waiver of any rights under this Agreement or of any cause of action arising out of the performance of this Agreement, and except as provided herein the Vendor shall be and remain liable in accordance with the terms of this Agreement and applicable law for all damages to the State caused by the Vendor's performance or failure to perform under this Agreement.

f. In the event of a breach of these representations and warranties, Vendor shall immediately, after telephonic notice from the State, begin work on curing such breaches. If it is necessary for Vendor to send at least one qualified and knowledgeable representative to the State's site where the system is located, this will be done at Vendor's sole expense. 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. In connection with the performance of this Agreement and the provision of services and deliverables under this Agreement, neither party will infringe any patent, copyright, trademark, trade secret or other proprietary right of any person. Neither party will improperly use any trade secrets or confidential or proprietary information owned by any third party in performing this

Agreement or the services related to this Agreement.

3. The Vendor represents and warrants that it has the full power and authority to grant the rights described in this Agreement without violating any rights of any third party, and that there is currently no actual or, to Vendor's knowledge, threatened suit by any such third party based on an alleged violation of such rights by Vendor. The Vendor further represents and warrants that the person executing this Agreement for Vendor has actual authority to bind Vendor to each and every term, condition and obligation to this Agreement, and that all requirements of Vendor have been fulfilled to provide such actual authority.

4. In accordance with Section 5 of this Agreement, Vendor will, at its expense, indemnify, defend and hold harmless State and its affiliates, and their respective successors and assigns, and their respective directors, officers and employees, from and against any and all claims, demands, suits, action and any and all damages, losses, liabilities, taxes, penalties, fines, charges, costs and expenses (including reasonable attorneys' fees) arising from or relating to a third party claim that any of the services or deliverables provided by Vendor to the State under this Agreement infringes that party's U.S. patent, U.S. trademark or copyright or misappropriates that party's trade secret or other intellectual property right, provided, however, Vendor shall not be required to indemnify State and its affiliates for any claims that result from or are related to: (i) the State's or other party's combination, operation, or use of the software in a manner not specifically authorized by Vendor; or (ii) alterations or modifications to the software not performed or authorized by Vendor.

If such a third party claim is made or appears likely to be made, Vendor, in its sole discretion, may elect: (i) to procure for State the right to continue to use the software product; (ii) to replace, at Vendor's cost, the software product, or any portion thereof, with a substitute product that functions substantially in accordance with the product's specifications; (iii) to modify the software product so that it does not infringe or misappropriate, provided that the product, as modified, continues to perform substantially in accordance with the applicable specifications.

Vendor's obligation to indemnify the State hereunder will be contingent on the State (i) notifying the Vendor in writing of the claim; (ii) allowing the Vendor the ability to control, and cooperating with Vendor in, the defense thereof and any related settlement negotiations; and (iii) in no event, agreeing to, or authorizing settlement of, any such claim without Vendor's prior written agreement, which such consent shall not be unreasonably withheld, conditioned or delayed. Vendor will reimburse State's reasonable out-of-pocket expenses incurred in providing assistance regarding any claim.

5. Vendor further represents and warrants that:

a. Vendor is an organization duly organized, validly existing and in good standing under the laws of its state of organization and has all requisite corporate power and authority to execute, deliver and perform its obligations under this Agreement;

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

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

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

e. Vendor's methods of accounting are consistent with Generally Accepted Accounting Principles (GAAP) and are capable of segregating costs by stage, segment, or cost objective in order to support change order accounting.

6. 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/.

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

By signing this agreement, the Vendor warrants that:

A. All known security issues are resolved.

B. Assistance will be provided to the State by the Vendor in performing an investigation to determine the nature of any security issues that are discovered or are reasonably suspected after acceptance. This investigation can include security scans made at the State's discretion. Failure by the Vendor to remedy any security issues discovered can be considered a breach of this agreement by the State

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/ are followed.

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

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 Vendor 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 Vendor's application depends is no longer supported, maintained, or patched by a qualified third party, the Vendor commits to migrate its application from that code base 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 Vendor 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 Vendor to work in good faith with the State toward a timely move to supported, maintained, and patched technology shall constitute a breach of this agreement and shall allow the State to cancel this agreement without penalty.

8. LICENSE TO PERFORM SECURITY SCANNING: The definitions immediately below apply to the following terms on security scanning.

- Security Scanning – the utilization of software tools to interrogate the application or hardware to assess compliance with standard best practices to preserve cyber security.

- Reverse Engineering – an action used to discover the content of application code.

- Application Code – the instruction utilized by a computer application to cause the computer to perform an instruction

The Vendor will provide the State, at a time and for duration agreeable to both parties, access to the application and underlying hardware referenced in this agreement for Security Scanning activities. Any scanning performed by the State will not be considered a violation of any licensure agreements the State has with the Vendor or the Vendor has with a third-party. Scanning by the State or any third-party acting for the State will not be considered reverse engineering. If the State Security Scanning efforts discover security issues the State may collaborate with, at the State discretion, the Vendor on remediation efforts, these remediation efforts will not be considered a violation of any licensure agreements the State has with the Vendor. The State while engaged, and after, with the Vendor on remediation will be indemnified and held harmless by the Vendor from all actions, lawsuits, damages (including all ordinary, incidental, consequential, and exemplary damages) or other proceedings that arise from security scanning, remediation efforts, or any after effects of security scanning or remediation. This indemnification includes all defense costs as well as reasonable attorneys' fees the State of South Dakota is required to pay in any such proceedings. The State will not be charged for any costs incurred by Vendor in these remediation efforts unless agreed to by the State in advance in writing. In the event of conflicting language this clause to supersede any other language in this or any other agreement made between the State and the Vendor.

9. SECURITY SCANNING: The State routinely applies security patches and security updates as needed to maintain compliance with industry best practices as well as state and federal audit requirements. Vendors who do business with the State must also subscribe to industry security

practices and requirements. Vendors 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 Vendor 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.

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

10. SECURE PRODUCT DEVELOPMENT: Consistent with the provisions of the agreement, the Vendor, subcontractor and or agent shall use the highest applicable industry standards for sound secure software development practices to resolve critical security issues as quickly as possible. These standards include but are not limited to the South Dakota Application Security Vulnerabilities document found at http://cybersecurity.sd.gov/docs/development/DevelopmentSecurityItems.pdf. Items listed under Section A of the South Dakota Security Vulnerabilities document may not be present in the software. Continued compliance to these standards is required as the standards will change over time. The "highest applicable industry standards" shall also be defined as the degree of care, skill, efficiency, and diligence that a prudent person possessing technical expertise in the subject area and acting in a like capacity would exercise in similar circumstances.

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

A. Name of the person responsible for certifying that all deliverables are secure.

B. Documentation detailing the vendor's version upgrading process (for those applications where there is or will be a maintenance agreement).

C. Notification of application patches and updates (for those applications where there is/will be a maintenance agreement).

D. List of tools used in the software development environment used to verify secure coding.

E. Based on a risk assessment, provide the State the secure configuration guidelines, specifications and requirements that describe security relevant configuration options and their implications for the overall security of the software. The guidelines, specifications and requirements must include descriptions of dependencies on the supporting platform,

including operating system, web server, application server and how they should be configured for security. The default configuration of the software shall be secure.

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

11. MALICIOUS CODE: The Vendor warrants that:

A. The software contains no code that does not support an application requirement.

B. Vendor will not insert into the software or any media on which the software is delivered any malicious or intentionally destructive code and

C. Vendor will use commercially reasonable efforts consistent with industry standards to scan for and remove any malicious code from the software before installation. In the event any malicious code is discovered in the software delivered by the Vendor, the Vendor shall provide the State at no charge with a copy of the applicable software that contains no malicious code or otherwise correct the affected portion of the services provided to the State. The remedies in this paragraph are in addition to other additional remedies available to the State

D. Will resolve all known security issues

12. 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. 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 Vendor'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 Vendor 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 Vendor if revealing the remedy will put the Vendor's intellectual property at risk. If the Vendor is unable to produce the project deliverables due to the Vendor actions or inactions within thirty (30) days of the application's denial of access or removal from production and the Vendor does not alter the project schedule or deliverables in writing within the same thirty (30) days then at the State's discretion the agreement may be terminated and Vendor is required to refund to the State the prorated contract amount.

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

14. 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 to fulfill licensing obligations and retains the right to use and upgrade as deemed appropriate its hypervisor and operating system technology and related hardware to execute the product 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.

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

16. USE OF ABSTRACTION TECHNOLOGIES:

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

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

17. THREAT NOTIFICATION: Upon becoming aware of a possible security threat(s) or exploit(s) with the Vendor's product(s) and or service(s) being used by the State the Vendor will notify the State within two (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).

18. SECURITY INCIDENT AND BREACH NOTIFICATION:

A. The Vendor, unless stipulated otherwise, shall notify the State Contact within 12 hours if the Vendor 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.

B. Notification to the State should include at a minimum all data available including: (i) Name of and contact information for the Vendor's Point of Contact for the security incident or data breach: (ii) date and time of the security incident or data breach; (iii) date and time the security incident or data breach was discovered: (iv) description of the security incident or data breach including the data involved, being as specific as possible; (v) potential number of records known, and if unknown the range of records; (vi) address

where the security incident or data breach occurred: and, (vii) the nature of the technologies involved. Notifications must be sent electronically and encrypted via NIST or other applicable federally approved encryption techniques. If there are none use AES-256 encryption with SHA-256 or SHA-2 hashing. Vendor shall use the term "data incident report" in the subject line of the email. If not all of the information is available for the notification within the specified time period Vendor shall provide the State with all of the available information.

19. HANDLING OF DATA BREACHES: If applicable, the Vendor 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 Vendor 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 Vendor will use a credit monitoring service, forensics company, advisors and public relations firm that are acceptable to the State, 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 Vendor shall inform the State of actions being taken or will be taken to reduce the risk of further loss to the State.

Except as otherwise required by law, the Vendor shall only provide notice of the incident to the State. The State will determine whether notification to the affected parties will (i) jeopardize the State's interests and (ii) be more appropriate for the Vendor to make. The method and content of the notification of the affected parties must be coordinated with, and is subject to, approval by the State. If the Vendor is required by federal law or regulation to conduct a security incident or data breach investigation, the results of the investigation must be reported to the State. If the Vendor is required by federal law or regulation to notify the affected parties, the State must also be notified.

Notwithstanding any other provision of this agreement, and in addition to any other remedies available to the State under law or equity, the Vendor will reimburse the State in full for all costs incurred by the State in investigation and remediation of the data breach including, but not limited, to providing notification to third parties whose data were compromised and to regulatory agencies or other entities as required by law or contract. The Vendor shall also reimburse the State in full for all costs the State incurs in its offering of 3 years credit monitoring to each person whose data were compromised. The Vendor shall also pay any and all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the data breach.

20. BROWSER: 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.

21. BACKUP COPIES: The State may make and keep backup copies of the software without additional cost or obligation on the condition that:

A. The State maintains possession of the backup copies.

B. The backup copies are used only as bona fide backups.

22. USE OF ABSTRACTION TECHNOLOGIES:

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

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

State of South Dakota

Appendix ___
Security and Vendor Questions

A = Data Center
B = Development
C = PMO Office
D = Telecommunications

	BIT Owner	Question	Response	Add text as required use "NA" when appropriate
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 host the system, is this an option?	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 _____ Java/JSP _____ MS SQL _____		
5.	A	Will the system support authentication? Does the system give 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	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	

		generated by the system using user-specific information such as last name or birthdate? If Yes to these, please explain		
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 Technology Security Policy which can be supplied upon request).	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 before they are finalized?	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 your proposed approach to software licenses.	Yes☐ No☐ NA ☐	
15.	B/C	Will the system provide an archival solution? If not is the State expected to develop a customized archival solution?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
16.	A	Will the system infrastructure have any processes that require scheduling?	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 be an issue?	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 as the State determines?	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 implementation of the system?	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 application?		
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 technology.		
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 affect the implementation of the system?	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 system?	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 the implementation of the system?	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 of the system?	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 implementation of the system?	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 implementation of the system?	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 of the system?	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 affect the implementation of the system?	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 of the system?	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 Access?	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 entire system?	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 the optional migrations?	Yes☐ No☐ NA ☐	
53.	A/B/ C/D	Will the system provide data encryption for sensitive information both in storage and transmission?	Yes☐ No☐ NA ☐	
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 when there are code changes, is this acceptable?	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 may be used as part of the vendor selection criteria. Is this acceptable?	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. Will this have a detrimental effect to the system?	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 State?	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 South Dakota?	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 updates?	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 this process?	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 applications?	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 transfer plan?	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 and by what percent?		
82.	B/C	Has your company ever integrated this product with an enterprise service bus to exchange data between diverse computing platforms?	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	Has your company ever developed a 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 implementation of the system?	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 details and provide full documentation as to the necessity of the requested access.		
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 environment?	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 to our data?	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	List any hardware or software you propose to use that is not state standard, the standards can be found at http://bit.sd.gov/standards/.		
96.	A	Please explain the pedigree of the software, include in your answer who are the people, organization and processes that created the software		
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 procedure.		

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 issues in the license agreement? Provide a brief explanation.	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 (brief summary response)?		
100.	B	Explain the use cases used for software assurance during development.		
101.	D	Describe the training your company offers related to defining security requirements, secure architecture and design, secure coding practices, and security testing.		
102.	D	Do you have developers that possess software security related certifications (e.g., the SANS secure coding certifications)?	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 and up-to date?	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 “custom” for a particular release?	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 assets processed?		
107.	D	In preparation for release, are undocumented functions in the software disabled, test/debug code removed, and source code comments sanitized?	Yes☐ No☐ NA ☐	
108.	A	Explain how and where the software validates (e.g., filter with white listing) inputs from untrusted sources before being used.		

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 damage possible by a successful attack?	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 data memory, and taint checking)?	Yes☐ No☐ NA ☐	
111.	D	How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used?		
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 party application(s) or system(s).	Yes☐ No☐ NA ☐	
113.	D	What security criteria, if any, are considered when selecting third-party suppliers?		
114.	B	What coding and/or API standards are used during development of the software?		
115.	B	What types of functional tests are/were performed on the software during its development (e.g., spot checking, component-level testing and integrated 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 distribution?		

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 sponsor conferences related to the software?		
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? How have the findings been mitigated?		
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 the security target and evaluation report available?	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? When in the SDLC are these scans performed? Are SwA experts involved in the analysis of the scan results?	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? Does it outline and establish a consistent and predictable support timeline?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
129.	A	How will patches and/or Service 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 released?		
132.	A	Can patches and Service Packs be uninstalled? Are the procedures for uninstalling a patch or Service Pack automated or manual?	Yes☐ No☐ NA ☐	
133.	A/B	How are reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, and prioritized?		
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 relation to deploying patches?		
136.	A	Are third-party developers contractually required to follow your configuration management policies?	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 used?		
138.	B	How is the software provenance verified (e.g. any checksums or signatures)?		
139.	A	Does your company publish a security section on its Web site? If so, do security researchers have the ability to report security issues?	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 mainstream requirements activities?		
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 to/for review?		
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 publicly accessible source.	Yes☐ No☐ NA ☐	
145.	B	Does the software use closed-source Application Programming Interfaces (APIs) that have undocumented functions?	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 events, provide examples of "trigger" events.	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 and on disk) in a vulnerable state?		
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 overridden?	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 weaknesses?	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 hardware? If yes, please describe.	Yes☐ No☐ NA ☐	

151.	A	What risk management measures are used during the software's design to mitigate risks posed by use of third-party components?		
152.	A	Does your company's defect classification scheme include security categories?	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 accreditation)?		
155.	A	Is a validation test suite or diagnostic available to validate that the application software is operating correctly and in a secure configuration following installation?	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 measures?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
157.	B	How is the assurance of software produced by third-party developers assessed?		
158.	D	How are trouble tickets submitted? How are support issues, specifically those that are security related, escalated?		
159.	A	Are help desk or support center personnel internal company resources or are these services outsourced to third parties?		
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 review?	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 ☐	

		development life cycle, explain.		
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 your company was subjected).		
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 they enforced?		
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 host server?		
170.	A	Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all registry settings?	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 of these scripts or agents?		
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 printed media?		
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 systems?	Yes☐ No☐ NA ☐	
180.	A/D	How are virus prevention, detection, correction, and updates handled for the products?		
181.	D	What type of firewalls (or application gateways) do you use? How are they monitored/managed?		
182.	D	What type of Intrusion Detection System/Intrusion Protection Systems (IDS/IPS) do you use? How are they monitored/managed?		
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 issues?	Yes☐ No☐ NA ☐	
185.	A	Do you have an automated security event management system?	Yes☐ No☐ NA ☐	
186.	A	What are your procedures for intrusion detection, incident response, and incident investigation/escalation?		

187.	A	Will you provide on-site support 24x7 to resolve security incidents?	Yes☐ No☐ NA ☐	
188.	A	Are security logs and audit trails protected from tampering or modification?	Yes☐ No☐ NA ☐	
189.	A	How do you control physical and electronic access to the log files? Are log files consolidated to single servers?		
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 or by a third party?	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 so please explain.	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 please explain.	Yes☐ No☐ NA ☐	
195.	A	How frequently is the security tests performed? Are the tests performed by internal resources or by a third party?		
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 redacted version is acceptable.	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 report?	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 copy of your assessment?	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 applications on other networks?	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)? c. Open Web Application Security Project (OWASP) Top Ten?	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 and to whom.		
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 to the contractual requirements?	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 risk assessment when are you planning on doing one?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	