Amendment to RFP #818 "24/7 Sobriety Program Monitoring Software RFP"

The South Dakota Attorney General's Office hereby amends RFP #818 to modify the following sections:

Section 1.7 "Schedule of Activities"

The section currently reads:

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

We would like to change the section to read:

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 by 11:59PM CST
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

Section 1.8 "Submitting your proposal"

The section currently reads:

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 by 11:59PM CST
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.

We would like to change the section to read:

All proposals must be completed and received in the SD ATG by electronic or hard copy submission by the date and time indicated in the Schedule of Activities. Proposals received after the deadline will be late and ineligible for consideration.

All proposals must be signed 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.

If submitting electronically, please send to the following email address: RFP818ATG247@state.sd.us

If submitting by hard copy, 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). 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.

Section 1.15 and 1.16 were repeated and need to be fixed:

The sections currently read:

1.15 SITE VISIT

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

1.16 PRESENTATIONS/DEMONSTRATIONS

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.

We would like to change the sections to read:

1.15 SITE VISIT

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

1.16 PRESENTATIONS/DEMONSTRATIONS

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.

1.17 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.

1.18 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.

Section 5.5 "DELIVERABLES"

The current section reads:

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.

We would like to change the section to read:

5.5.10 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.

Appendix C – Included I/T Contract Terms and Conditions – Vendor Hosted Proposal Contract Exhibit B Clauses 15, 22 and 23

The Current section reads:

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.

We would like to change the section to read:

15. Scanning and Audit Authorization

The Consultant will provide the State at no cost and at a date, time and for duration agreeable to both parties, authorization to scan and access to a test system containing test data for security scanning activities. The system and data provided to the State by Consultant 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. Consultant 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 Consultant or that the consultant has with a third-party.

The Consultant will also allow the State at the State's expense, not to include Consultant's expenses, to perform up to two security audit and vulnerability assessments per year to provide verification of Consultant's IT security safeguards for the system and its data. The State will work with the Consultant to arrange the audit at a time least likely to create workload issues for the Consultant and will accept scanning a test or UAT environment on which the code and systems are a mirror image of the production environment.

The Consultant indemnifies the state for ordinary, consequential and incidental damages to the Consultant'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, at the State's discretion with, the Consultant on remediation efforts. These remediation efforts will not be considered a violation of any licensure agreements between the State and Consultant. The State while engaged, and after, with the Consultant 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, and 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 consultant in these remediation efforts unless agreed to by the State in advance in writing. In the event of conflicting language this clause supersedes any other language in this or any other agreement made between the State and the Consultant.

The Consultant agrees to work with the State to rectify any serious security issues revealed by the security audit and or security scanning. This includes additional security audits and security scanning that shall be performed after any remediation efforts to confirm the security issues have been resolved and no further security issues exist.

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. 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.

23. 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.

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. 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.

34. 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.

35. 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.

All other sections and provisions of the RFP remain intact as posted.

Any and all questions should be posed by email to RFP818ATG247@state.sd.us

Dated: January 12, 2017