STATE OF MICHIGAN
ENTERPRISE PROCUREMENT

Department of Technology Management and Budget
525 W. Allegan St., Lansing, Michigan 48913
P.O. Box 30026 Lansing, Michigan 48909

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **171 180000000201**
between
THE STATE OF MICHIGAN
and

CONTRACTOR	
	STACS DNA Inc.
	2255 St Laurent Blvd., Suite 206
	Ottawa, ON K1G 4K3
	Jocelyn Tremblay
	613-274-7822 x2000
	jocelyn.tremblay@stacsdna.com
	*******7331

STATE			
	Program Manager	Nancy Becker Bennett	MSP
		517-284-3205	
		BeckerN@michigan.gov	
	Contract Administrator	Timothy Taylor	DTMB
		517-284-7006	
		Taylort27@michigan.gov	

CONTRACT SUMMARY			
DESCRIPTION: Sexual Assault Evidence Kits			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW**
January 22, 2018	January 21, 2023	(2) 5-Year	
PAYMENT TERMS		**DELIVERY TIMEFRAME**	
Net 45		N/A	
ALTERNATE PAYMENT OPTIONS			**EXTENDED PURCHASING**
☐ P-card ☐ Direct Voucher (DV) ☐ Other			☐ Yes ☒ No
MINIMUM DELIVERY REQUIREMENTS			
N/A			
MISCELLANEOUS INFORMATION			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION			**$3,576,701.03**

FOR THE CONTRACTOR:

Company Name

Authorized Agent Signature

Authorized Agent (Print or Type)

Date

FOR THE STATE:

Signature

Name & Title

Agency

Date

STATE OF MICHIGAN

This Hosted Software Contract (this "**Contract**") is agreed to between the State of Michigan (the "**State**") and STACS DNA, Inc. ("**Contractor**"). This Contract is effective on January 22, 2018 ("**Effective Date**"), and unless earlier terminated, will expire on January 21, 2023 (the "Term").

This Contract may be renewed for up to two (2) additional five (5) year periods. Renewal must be by written notice from the State and will automatically extend the Term of this Contract.

1. **Definitions**. For the purposes of this Contract, the following terms have the following meanings:

"**Acceptance**" has the meaning set forth in **Section 13.5**.

"**Acceptance Tests**" means such tests as may be conducted in accordance with **Section 13** and the Statement of Work to determine whether the Software meets the material requirements of this Contract and the Documentation.

"**Affiliate**" of a Person means any other Person that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Person. For purposes of this definition, the term "control" (including the terms "controlled by" and "under common control with") means the direct or indirect ownership of more than fifty percent (50%) of the voting securities of a Person.

"**Allegedly Infringing Materials**" has the meaning set forth in **Section 27.3(b)(ii)**.

"**API**" means all Application Programming Interfaces and associated API Documentation that is specific to the State's information technology infrastructure and custom developed and provided by Contractor, and as updated from time to time, to allow the Software to integrate with Contractor's Software and various Third-Party Software or State developed software.

"**Authorized Users**" means all Persons authorized by the State to access and use the Software in connection with this Contract.

"**Business Day**" means a day other than a Saturday, Sunday or other day on which the State is authorized or required by Law to be closed for business.

"Business Owner" is the individual appointed by the State to (a) act as the State's representative in all matters relating to the Contract, and (b) co-sign off on notice of Acceptance for the Software. The Business Owner will be identified in the Statement of Work.

"**Business Requirements Specification**" means the initial specification setting forth the State's business requirements regarding the features and functionality of the Software, as set forth in the Statement of Work.

"**Change**" has the meaning set forth in **Section 3.2**.

"**Change Notice**" has the meaning set forth in **Section 3.2(b)**.

"**Change Proposal**" has the meaning set forth in **Section 3.2(a)**.

"**Change Request**" has the meaning set forth in **Section 3.2**.

"**Confidential Information**" has the meaning set forth in **Section 21.1**.

"**Configuration**" means State-specific changes made by the Contractor to the Software without Source Code or structural data model changes occurring.

"**Contract**" has the meaning set forth in the preamble.

"**Contract Administrator**" is the individual appointed by each party to (a) administer the terms of this Contract, and (b) approve any Change Notices under this Contract. Each party's Contract Administrator will be identified in the Statement of Work.

"**Contractor**" has the meaning set forth in the preamble.

"**Contractor's Bid Response**" means the Contractor's proposal submitted in response to the RFP.

"**Contractor Personnel**" means all employees and independent contractors of Contractor or any Permitted Subcontractors involved in the performance of Services hereunder.

"**Contractor's Test Package**" has the meaning set forth in **Section 12.2**.

"**Customization**" means State-specific changes made by Contractor to the Software requiring changes to the Source Code.

"**Deliverables**" as further expressly described herein means the Software offered as hosted Services, and all other documents and other materials that Contractor is required to or otherwise does provide to the State under this Contract and otherwise in connection with any Services, including all items specifically identified as Deliverables in the Statement of Work.

"**Dispute Resolution Procedure**" has the meaning set forth in **Section 31.1**.

"**Documentation**" means user manuals, operating manuals, technical manuals and any other instructions, specifications, documents or materials, in any form or media, that describe the functionality, installation, testing, operation, use, maintenance, support, technical or other components, features or requirements of the Software.

"**Effective Date**" has the meaning set forth in the preamble.

"**Fees**" means collectively, the License Fees, Implementation Fees, and Support Services Fees.

"**Financial Audit Period**" has the meaning set forth in **Section 29.1**.

"**Force Majeure**" has the meaning set forth in **Section 32.1**.

"**Harmful Code**" means any: (a) virus, trojan horse, worm, backdoor or other software or hardware devices the effect of which is to permit unauthorized access to, or to disable, erase, or otherwise harm, any computer, systems or software; or (b) time bomb, drop dead device, or other software or hardware device designed to disable a computer program automatically with the passage of time or under the positive control of any Person, or otherwise prevent, restrict or impede the State's or any Authorized User's use of such software.

"**HIPAA**" has the meaning set forth in **Section 20.1**.

"**Hosting Environment**" means, collectively, the Microsoft Azure Government platform, environment and conditions on, in or under which the Software is intended to be installed and operate, as set forth in the Statement of Work, including such structural, functional and other features, conditions and components as hardware, operating software and system architecture and configuration.

"**Implementation Fees**" has the meaning set forth in **Section 17.2**.

"**Implementation Plan**" means the schedule included in the Statement of Work setting forth the sequence of events for the performance of Services under the Statement of Work, including the Milestones and Milestone Dates.

"**Integration Testing**" has the meaning set forth in **Section 13.1(c)**.

"**Intellectual Property Rights**" means all or any of the following: (a) patents, patent disclosures, and inventions (whether patentable or not); (b) trademarks, service marks, trade dress, trade names, logos, corporate names, and domain names, together with all of the associated goodwill; (c) copyrights and copyrightable works (including computer programs), mask works and rights in data and databases; (d) trade secrets, know-how and other confidential information; and (e) all other intellectual property rights, in each case whether registered or unregistered and including all applications for, and renewals or extensions of, such rights, and all similar or equivalent rights or forms of protection provided by applicable Law in any jurisdiction throughout the world.

"**Key Personnel**" means any Contractor Personnel identified as key personnel in the Statement of Work.

"**Law**" means any statute, law, ordinance, regulation, rule, code, order, constitution, treaty, common law, judgment, decree or other requirement or rule of any federal, state, local or foreign government or political subdivision thereof, or any arbitrator, court or tribunal of competent jurisdiction having force of law.

"**License**" means Contractor's license grant to the State and its Authorized Users as set forth in **Section 4**.

"**License Fee**" has the meaning set forth in **Section 17.1**.

"**Loss or Losses**" means all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable outside attorneys' fees and the third party costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers.

"**Maintenance Release**" means any update, upgrade, release or other adaptation or modification of the Software, including any updated Documentation, that Contractor may generally provide or make available to its licensees from time to time during the Term, which may contain, among other things, error corrections, enhancements, improvements or other changes to the user interface, functionality, compatibility, capabilities, performance, efficiency or quality of the Software.

"**Milestone**" means an event or task described in the Implementation Plan under the Statement of Work that must be completed by the corresponding Milestone Date.

"**Milestone Date**" means the date by which a particular Milestone must be completed as set forth in the Implementation Plan under the Statement of Work.

"**New Version**" means any new version of the Software that the Contractor may from time to time introduce and market generally as a distinct licensed product, as may be indicated by Contractor's designation of a new version number.

"**Nonconformity**" or **"Nonconformities"** means any material failure or failures of the Software to conform to the requirements of this Contract, including any applicable Documentation.

"**Open-Source Components**" means any software component that is subject to any open-source copyright license agreement, including any GNU General Public License or GNU Library or Lesser Public License, or other obligation, restriction or license agreement that substantially conforms to the Open Source Definition as prescribed by the Open Source Initiative or otherwise may require disclosure or licensing to any third party of any source code with which such software component is used or compiled.

"**Open-Source License**" has the meaning set forth in **Section 5**.

"**Permitted Subcontractor**" has the meaning set forth in **Section 10.4**.

"**Person**" means an individual, corporation, partnership, joint venture, limited liability company, governmental authority, unincorporated organization, trust, association or other entity.

"**Pricing**" means any and all fees, rates and prices payable under this Contract, including pursuant to any Schedule or Exhibit hereto.

"**Pricing Schedule**" means the schedule attached as **Schedule D**, setting forth the License Fees, Implementation Fees, Support Services Fees, and any other fees, rates and prices payable under this Contract.

"**Project Manager**" is the individual appointed by each party to (a) monitor and coordinate the day-to-day activities of this Contract, and (b) for the State, to co-sign off on its notice of Acceptance for the Software. Each party's Project Manager will be identified in the Statement of Work.

"**Representatives**" means a party's employees, officers, directors, partners, shareholders, agents, attorneys, successors and permitted assigns.

"**RFP**" means the State's request for proposal designed to solicit responses for Services under this Contract.

"**State**" has the meaning set forth in the preamble.

"**State Data**" has the meaning set forth in **Section 20.1**.

"**State Materials**" means all materials and information, including documents, data, know-how, ideas, methodologies, specifications, software, content and technology, in any form or media, directly or indirectly provided or made available to Contractor by or on behalf of the State in connection with this Contract.

"**State Resources**" has the meaning set forth in **Section 11.1(a)**.

"**Services**" means any of the services Contractor is required to or otherwise does provide under this Contract, the Statement of Work, and the Service Level Agreement.

"**Service Level Agreement**" means the service level agreement attached as **Schedule B** to this Contract, setting forth Contractor's obligations with respect to the hosting, management and operation of the Software.

"**Site**" means the physical location designated by Contractor for delivery and installation of the Software.

"**Software**" means Contractor's software in the hosted environment set forth in the Statement of Work, and any Maintenance Releases or New Versions provided to the State and any Customizations,

Configurations made by or for the State pursuant to this Contract, and all copies of the foregoing permitted under this Contract and the License Agreement.

"**Source Code**" means the human readable source code of the Software to which it relates, in the programming language in which the Software was written, together with all related flow charts and technical documentation, including a description of the procedure for generating object code, all of a level sufficient to enable a programmer reasonably fluent in such programming language to provide maintenance for the Software.

"**Specifications**" means, for the Software, the specifications collectively set forth in the Business Requirements Specification, Technical Specification, and Documentation for such Software, or elsewhere in the Statement of Work.

"**Statement of Work**" means the statement of work entered into by the parties and attached as **Schedule A** to this Contract.

"**Stop Work Order**" has the meaning set forth in **Section 25**.

"**Support Services**" means the Software maintenance and support services Contractor is required to or otherwise does provide to the State under the Service Level Agreement.

"**Support Services Fees**" has the meaning set forth in **Section 17.3**.

"**Technical Specification**" means, with respect to any Software, the document setting forth the technical specifications for such Software and included in the Statement of Work.

"**Term**" has the meaning set forth in the preamble.

"**Test Data**" has the meaning set forth in **Section 12.2**.

"**Testing Period**" has the meaning set forth in **Section 13.1(b)**.

"**Test Results**" has the meaning set forth in **Section 12.2**.

"**Third Party**" means any Person other than the State or Contractor.

"**Third Party License**" has the meaning set forth in **Section 5**.

"**Third-Party Software**" means software, content, and technology, in any form or media, in which any Person other than the State or Contractor owns any Intellectual Property Right, but excluding Open-Source Components.

"**Transition Period**" has the meaning set forth in **Section 24.3**

"**Transition Responsibilities**" has the meaning set forth in **Section 24.3**.

"**Unauthorized Removal**" has the meaning set forth in **Section 10.3(b)**.

"**Unauthorized Removal Credit**" has the meaning set forth in **Section 10.3(c)**.

"**User Data**" means all data, information and other content of any type and in any format, medium or form, whether audio, visual, digital, screen, GUI or other, that is input, uploaded to, placed into or collected, stored, processed, generated or output by any device, system or network by the State except that User Data does not include the Software, Documentation, Services, Deliverables, or data, information or content, including any GUI, audio, visual or digital or other display or output, that is generated automatically upon executing the Software without additional user input.

"**Work Product**" means all State-specific deliverables that Contractor is required to, or otherwise does, provide to the State under this Contract including but not limited to APIs, computer scripts, macros, user interfaces, reports, project management documents, forms, templates, and other State-specific documents and related materials together with all ideas, concepts, processes, and methodologies developed in connection with this Contract whether or not embodied in this Contract. Work Product does not include the Software.

2. Schedules. All Schedules that are referenced herein and attached hereto are hereby incorporated by reference. The following Schedules are attached hereto and incorporated herein:

Schedule A	Statement of Work
Schedule B	Service Level Agreement
Schedule C	License Agreement – Not applicable
Schedule D	Pricing Schedule
Schedule E	Disaster Recovery Plan-Confidential
Schedule F	Data Security Terms

3. Statement of Work. Contractor shall provide Services and Deliverables pursuant to the executed Statement of Work entered into under this Contract. The Statement of Work shall not be effective unless signed by each party's Contract Administrator. The term of the Statement of Work shall commence on the parties' full execution of the Statement of Work and terminate upon the earlier of: (i) when the parties have fully performed their obligations, or (ii) upon the natural expiration or earlier termination of this Contract. The terms and conditions of this Contract will apply at all times to the Statement of Work. The State shall have the right to terminate such Statement of Work as set forth in **Section 24**. Contractor acknowledges that time is of the essence with respect to Contractor's obligations under the Statement of Work and agrees that prompt and timely performance of all such obligations in accordance with this Contract and the Statement of Work (including the Implementation Plan and all Milestone Dates) is strictly required.

3.1 Statement of Work Requirements. The Statement of Work will include the following:

(a) names and contact information for Contractor's Contract Administrator, Project Manager and Key Personnel;

(b) names and contact information for the State's Contract Administrator, Project Manager and Business Owner;

(c) a detailed description of the Services to be provided under this Contract, including any training obligations of Contractor;

(d) a detailed description of the Software to be provided under this Contract, including the:

(i) version and release number of the Software;

(ii) Business Requirements Specification;

(iii) Technical Specification;

(iv) The Hosting Environment; and

(v) a description of the Documentation to be provided;

(e) the Project Management Methodology (PMM) that will be utilized;

(f) an Implementation Plan that follows the PMM, including all Milestones, the corresponding Milestone Dates and the parties' respective responsibilities under the Implementation Plan;

(g) the due dates for payment of Fees and any invoicing requirements, including any Milestones on which any such Fees are conditioned, and such other information as the parties deem necessary;

(h) disclosure of all Third-Party Software and Open-Source Components (each identified on a separate exhibit to the Statement of Work), in each case accompanied by such related documents as may be required by this Contract;

(i) a detailed description of all State Resources required to complete the Implementation Plan.

3.2 Change Control Process. The State may at any time request in writing (each, a "**Change Request**") changes to the Statement of Work, including changes to the Services and Implementation Plan (each, a "**Change**"). Upon the State's submission of a Change Request, the parties will evaluate and implement all mutually agreed upon Changes in accordance with this **Section 3.2**.

(a) As soon as reasonably practicable, and in any case within twenty (20) Business Days following receipt of a Change Request, Contractor will provide the State with a written proposal for implementing the requested Change ("**Change Proposal**"), setting forth:

(i) a written description of the proposed Changes to any Services or Deliverables;

(ii) an amended Implementation Plan reflecting: (A) the schedule for commencing and completing any additional or modified Services or Deliverables; and (B) the effect of such Changes, if any, on completing any other Services under the Statement of Work;

(iii) any additional State Resources Contractor deems necessary to carry out such Changes; and

(iv) any increase or decrease in Fees resulting from the proposed Changes, which increase or decrease will reflect any increase or decrease in time and expenses Contractor requires to carry out the Change.

(b) Within thirty (30) Business Days following the State's receipt of a Change Proposal, the State will by written notice to Contractor, approve, reject, or propose modifications to such Change Proposal. If the State proposes modifications, Contractor must modify and re-deliver the Change Proposal reflecting such modifications, or notify the State of any disagreement, in which event the parties will negotiate in good faith to resolve their disagreement. Upon the State's approval of the Change Proposal or the parties' agreement on all proposed modifications, as the case may be, the parties will execute a written agreement to the Change Proposal ("**Change Notice**"), which Change Notice will be signed by the State's Contract Administrator and will constitute an amendment to the Statement of Work to which it relates; and

(c) If the parties fail to enter into a Change Notice within fifteen (15) Business Days following the State's response to a Change Proposal, the State may, in its discretion:

(i) require Contractor to perform the Services under the Statement of Work without the Change;

(ii) require Contractor to continue to negotiate a Change Notice;

(iii) initiate a Dispute Resolution Procedure; or

(iv) notwithstanding any provision to the contrary in the Statement of Work, terminate this Contract under **Section 24.2**.

(d) No Change will be effective until the parties have executed a Change Notice. Except as the State may request in its Change Request or otherwise in writing, Contractor must continue to perform its obligations in accordance with the Statement of Work pending negotiation and execution of a Change Notice. Contractor will use its best commercial efforts to limit any delays or Fee increases from any

Change to those necessary to perform the Change in accordance with the applicable Change Notice. Each party is responsible for its own costs and expenses of preparing, evaluating, negotiating, and otherwise processing any Change Request, Change Proposal, and Change Notice.

(e) The performance of any functions, activities, tasks, obligations, roles and responsibilities comprising the Services as described in this Contract are considered part of the Services and, thus, will not be considered a Change. This includes the delivery of all Deliverables in accordance with their respective Specifications, and the diagnosis and correction of Non-Conformities discovered in Deliverables prior to their Acceptance by the State or, subsequent to their Acceptance by the State, as necessary for Contractor to fulfill its associated warranty requirements and its Support Services under this Contract.

(f) Contractor may, on its own initiative and at its own expense, prepare and submit its own Change Request to the State. However, the State will be under no obligation to approve or otherwise respond to a Change Request initiated by Contractor.

4. Contractor Software License. Contractor hereby grants to the State (including all constituent agencies or Departments) and its unlimited Authorized Users the non-exclusive, non-transferable and non-sublicensable right and license to use the Software and Documentation in the User Acceptance Testing, Training, and Production environments, in accordance with the terms and conditions of this Contract. Without waiving any claims or defenses, including Governmental Immunity, the State shall be liable for a breach of this license grant by any constituent agencies or Departments under this Agreement; provided, however, that the State shall not be liable for a breach by any non-affiliated Authorized Users.

5. Third-Party Software Licenses. Any use hereunder of Third-Party Software shall be governed by, and subject to, the terms and conditions of the applicable Third-Party Software license agreement ("**Third-Party License**"). As of the effective date of this Contract, Contractor shall identify and describe in an exhibit to the Statement of Work any Third-Party Software being used in connection with the Services.

6. Open-Source Licenses. Any use hereunder of Open-Source Components shall be governed by, and subject to, the terms and conditions of the applicable open-source license ("**Open-Source License**"). As of the effective date of this Contract, Contractor shall identify and describe in an exhibit to the Statement of Work each of the Open-Source Components of the Software, and include an exhibit attaching all applicable Open-Source Software Licenses or identifying the URL where these licenses are publicly available.

7. Software Implementation.

7.1 Implementation. Contractor will deliver, install, configure, integrate, and otherwise provide and make fully operational the Software on or prior to the applicable Milestone Date in accordance with the express criteria set forth in the Statement of Work.

7.2 Site Preparation. Contractor is responsible for ensuring the relevant Hosting Environment is set up and in working order to allow Contractor to deliver and install the Software on or prior to the applicable

Milestone Date. Contractor will provide the State with such notice as is specified in the Statement of Work, prior to installation of the Software, to give the State sufficient time to prepare for purposes of end user acceptance testing.

8. Hosting and Support.

8.1 Availability. Contractor will maintain the Availability Requirement set forth in the Service Level Agreement attached as **Schedule B** to this Contract.

8.2 Support Services. Contractor shall provide the State with the Support Services and maintain the Support Service Level Requirement set forth in the Service Level Agreement attached as **Schedule B** to this Contract.

9. Data Privacy and Information Security.

9.1 Undertaking by Contractor. Contractor shall comply with all security requirements set forth in the Data Security Schedule, attached as **Schedule F** to this Contract. In addition, and without limiting Contractor's obligation of confidentiality as further described, Contractor is responsible for establishing and maintaining a data privacy and information security program, including physical, technical, administrative, and organizational safeguards, that is designed to: (a) ensure the security and confidentiality of the State Data; (b) protect against any anticipated threats or hazards to the security or integrity of the State Data; (c) protect against unauthorized disclosure, access to, or use of the State Data; (d) ensure the proper disposal of State Data; and (e) ensure that all Contractor Representatives comply with all of the foregoing.

9.2 To the extent that Contractor has access to the State's computer system, Contractor must comply with the State's Acceptable Use Policy, see http://michigan.gov/cybersecurity/0,1607,7-217-34395_34476---,00.html. All Contractor Personnel will be required, in writing, to agree to the State's Acceptable Use Policy before accessing the State's system. The State reserves the right to terminate Contractor's access to the State's system if a violation occurs.

9.3 Right of Audit by the State. Without limiting any other audit rights of the State, the State has the right to review Contractor's data privacy and information security program prior to the commencement of Services and from time to time during the term of this Contract to ensure compliance with the Contractor's data privacy and information security obligations pursuant to the terms of this Contract. . During the providing of Services, on an ongoing basis from time to time and with seven (7) days notice, the State, at its own expense, is entitled to perform, or to have performed, an on-site audit of Contractor's data privacy and information security program. The use by the State of any authorized representative to conduct any such audit shall be subject to and conditional upon such authorized representative executing a confidentiality agreement consistent with the confidentiality obligations set forth in this Agreement. In lieu of an on-site audit, upon request by the State, Contractor agrees to complete, within forty-five (45) calendar days of receipt, an audit questionnaire provided by the State regarding Contractor's data privacy and information security program.

9.4 Audit Findings. With respect to State Data, Contractor must implement any reasonably required safeguards as identified by the State or by any audit of Contractor's data privacy and information security program. To the extent any such safeguards require Contractor as a result in a material change in scope to the Services, Contractor shall inform the State Contract Administrator in writing and the parties will follow the Change control process in Section 2.2 of this Contract.

9.5 State's Right to Termination for Deficiencies. The State reserves the right, at its sole election, to immediately terminate this Contract or the Statement of Work without limitation and without liability if the Contractor fails or has failed to meet its material obligations under this **Section 9** and does not cure such failure within thirty (30) days of the State's written notice of deficiencies under this Section.

10. Performance of Services. Contractor will provide all Services and Deliverables in a timely, professional and workmanlike manner and in accordance with the terms, conditions, and Specifications set forth in this Contract and the Statement of Work.

10.1 Contractor Personnel.

(a) Contractor is solely responsible for all Contractor Personnel and for the payment of their compensation, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits.

(b) Prior to any Contractor Personnel performing any Services, Contractor will:

(i) ensure that such Contractor Personnel have the legal right to work in the United States;

(ii) upon request, require such Contractor Personnel to execute written agreements, in form and substance acceptable to the State, that bind such Contractor Personnel to confidentiality provisions that are at least as protective of the State's information (including all Confidential Information) as those contained in this Contract; and

(iii) upon request, perform background checks on all Contractor Personnel who have access to State Data prior to their assignment. The scope is at the discretion of the State and documentation must be provided as requested. Contractor is responsible for all costs associated with the requested background checks. The State, in its sole discretion, may also perform background checks on Contractor Personnel.

(c) Contractor and all Contractor Personnel will comply with all rules, regulations, and policies of the State that are communicated to Contractor in writing, including security procedures concerning systems and data and remote access, building security procedures, including the restriction of access by the State to certain areas of its premises or systems, and general health and safety practices and procedures.

(d) The State reserves the right to require the removal of any Contractor Personnel found, in the judgment of the State, to be unacceptable. The State's request must be written with reasonable detail outlining the reasons for the removal request. Replacement personnel for the removed person must be fully qualified for the position. If the State exercises this right, and Contractor cannot immediately replace the removed personnel, the State agrees to negotiate an equitable adjustment in schedule or other terms that may be affected by the State's required removal.

10.2 Contractor's Project Manager. Throughout the Term of this Contract, Contractor must maintain a Contractor employee acceptable to the State to serve as Contractor's Project Manager, who will be considered Key Personnel of Contractor. Contractor's Project Manager will be identified in the Statement of Work.

(a) Contractor's Project Manager must:

(i) have the requisite authority, and necessary skill, experience, and qualifications, to perform in such capacity;

(ii) be responsible for overall management and supervision of Contractor's performance under this Contract; and

(iii) be the State's primary point of contact for communications with respect to this Contract, including with respect to giving and receiving all day-to-day approvals and consents.

(b) Contractor's Project Manager [or her/his designee if unavailable (e.g. due to illness, disability, etc.)] must attend all regularly scheduled meetings as set forth in the Implementation Plan, and will otherwise be available as set forth in the Statement of Work.

(c) Contractor will maintain the same Project Manager throughout the Term of this Contract, unless:

(i) the State requests in writing the removal of Contractor's Project Manager;

(ii) the State consents in writing to any removal requested by Contractor in writing;

(iii) Contractor's Project Manager ceases to be employed by Contractor, whether by resignation, involuntary termination or otherwise.

(d) Contractor will promptly replace its Project Manager on the occurrence of any event set forth in **Section 10.2(c)**. Such replacement will be subject to the State's prior written approval.

10.3 Contractor's Key Personnel.

(a) The State has the right to recommend and approve in writing the initial assignment, as well as any proposed reassignment or replacement, of any Key Personnel. Before assigning an individual to

any Key Personnel position, Contractor will notify the State of the proposed assignment, introduce the individual to the State's Project Manager, and provide the State with a resume and any other information about the individual reasonably requested by the State. The State reserves the right to interview the individual before granting written approval. In the event the State finds a proposed individual unacceptable, the State will provide a written explanation including reasonable detail outlining the reasons for the rejection.

(b) Contractor will not remove any Key Personnel from their assigned roles on this Contract without the prior written consent of the State. The Contractor's removal of Key Personnel without the prior written consent of the State is an unauthorized removal ("**Unauthorized Removal**"). An Unauthorized Removal does not include replacing Key Personnel for reasons beyond the reasonable control of Contractor, including illness, disability, leave of absence, personal emergency circumstances, resignation, or for cause termination of the Key Personnel's employment.

(c) It is further acknowledged that an Unauthorized Removal may interfere with the timely and proper completion of this Contract, to the potential loss and damage of the State, and that it would be impracticable and extremely difficult to fix the actual damage sustained by the State as a result of any Unauthorized Removal. Therefore, Contractor and the State agree that in the case of any Unauthorized Removal in respect of which the State does not elect to exercise its rights under **Section 24.1**, Contractor will issue to the State an amount equal to $10,000 per individual (each, an "**Unauthorized Removal Credit**").

(d) Contractor acknowledges and agrees that each of the Unauthorized Removal Credits assessed under **Subsection (c)** above: (i) is a reasonable estimate of and compensation for the anticipated or actual harm to the State that may arise from the Unauthorized Removal, which would be impossible or very difficult to accurately estimate; and (ii) may, at the State's option, be credited or set off against any Fees or other charges payable to Contractor under this Contract.

10.4 Subcontractors. Contractor will not, without the prior written approval of the State, which consent may be given or withheld in the State's sole discretion, engage any Third Party to perform Services. The State's approval of any such Third Party (each approved Third Party, a "**Permitted Subcontractor**") does not relieve Contractor of its representations, warranties or obligations under this Contract. The parties acknowledge that any Subcontractors identified within the SOW will be deemed approved. Without limiting the foregoing, Contractor will:

(a) be responsible and liable for the acts and omissions of each such Permitted Subcontractor (including such Permitted Subcontractor's employees who, to the extent providing Services or Deliverables, shall be deemed Contractor Personnel) to the same extent as if such acts or omissions were by Contractor or its employees;

(b) be responsible for all fees and expenses payable to, by or on behalf of each Permitted Subcontractor in connection with this Contract, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits; and

(c) notify the State of the location of the Permitted Subcontractor and indicate if it is located within the continental United States.

11. State Obligations.

11.1 State Resources and Access. The State is responsible for:

(a) providing the State Materials and such other resources as may be specified in the Statement of Work (collectively, "**State Resources**"); and

(b) providing Contractor Personnel with such access to State facilities as is necessary for Contractor to perform its obligations on a timely basis as set forth in the Statement of Work.

11.2 State Project Manager. Throughout the Term of this Contract, the State will maintain a State employee to serve as the State's Project Manager under this Contract. The State's Project Manager will be identified in the Statement of Work. The State's Project Manager will be available as set forth in the Statement of Work.

12. Pre-Delivery Testing.

12.1 Testing By Contractor. Before delivering and installing the Software, Contractor must:

(a) test the Software to confirm that it is fully operable, meets all applicable Specifications and will function in accordance with the Specifications and Documentation when properly installed in the Hosting Environment;

(b) scan the Software using industry standard scanning software and definitions to confirm it is free of Harmful Code; and

(c) remedy any Non-Conformity or Harmful Code identified and retest and rescan the Software.

12.2 Test Data and Results. Unless otherwise specified in the Statement of Work, Contractor shall provide to the State all test data and testing scripts used by Contractor for its pre-delivery testing ("**Test Data**"), together with the results Contractor expects to be achieved by processing the Test Data using the Software ("**Test Results**," and together with Test Data, "**Contractor's Test Package**").

13. Acceptance Testing; Acceptance. Unless otherwise set forth in the Statement of Work, the following Section will control Acceptance Testing of the Software:

13.1 Acceptance Testing.

(a) Unless otherwise specified in the Statement of Work, upon installation of the Software, Acceptance Tests will be conducted as set forth in this **Section 13** to ensure the Software conforms to the requirements of this Contract, including the applicable Specifications and Documentation. The State may, but is not obligated, to perform its own pretest on the Software utilizing Contractor's Test Package.

If the State does perform a pretest, and Contractor's Test Package does not successfully pass the Test Data or Test Results scripts as described by Contractor, the State, at its discretion, is not obligated to move into the formal Acceptance Tests set forth in this Section. The State may elect to send Contractor's Test Package back to Contractor to correct any problems encountered with the Test Data or Test Results.

(b) All Acceptance Tests will take place at the designated Site(s) in the Hosting Environment described in the Statement of Work, commence on the Business Day following installation of the Software and be conducted diligently for up to fifteen (15) Business Days, or such other period as may be set forth in the Statement of Work (the "**Testing Period**"). Acceptance Tests will be conducted by the party responsible as set forth in the Statement of Work or, if the Statement of Work does not specify, the State, provided that:

(i) for Acceptance Tests conducted by the State, if requested by the State, Contractor will make suitable Contractor Personnel available to observe or participate in such Acceptance Tests; and

(ii) for Acceptance Tests conducted by Contractor, the State has the right to observe or participate in all or any part of such Acceptance Tests.

Contractor is solely responsible for all costs and expenses related to Contractor's performance of, participation in, and observation of Acceptance Testing.

(c) Upon delivery and installation of any Customization, Configuration or API to the Software under the Statement of Work, additional Acceptance Tests will be performed on the configured Software as a whole to ensure full operability, integration, and compatibility among all elements of the Software ("**Integration Testing**"). Integration Testing is subject to all procedural and other terms and conditions set forth in **Section 13.1**, **Section 13.3**, and **Section 13.4**.

(d) The State may suspend Acceptance Tests and the corresponding Testing Period by written notice to Contractor if the State discovers a material Non-Conformity in the tested Software or part or feature of the Software. In such event, Contractor will immediately, and in any case within ten (10) Business Days, use its reasonable efforts to correct such Non-Conformity, whereupon the Acceptance Tests and Testing Period will resume for the balance of the Testing Period.

13.2 Notices of Completion, Non-Conformities, and Acceptance. Within fifteen (15) Business Days following the completion of any Acceptance Tests, including any Integration Testing, the party responsible for conducting the tests will prepare and provide to the other party written notice of the completion of the tests. Such notice must include a report describing in reasonable detail the tests conducted and the results of such tests, including any uncorrected Non-Conformity in the tested Software.

(a) If such notice is provided by either party and identifies any Non-Conformities, the parties' rights, remedies, and obligations will be as set forth in **Section 13.3** and **Section 13.4**.

(b) If such notice is provided by the State, is signed by the State's Business Owner and Project Manager, and identifies no Non-Conformities, such notice constitutes the State's Acceptance of such Software.

(c) If such notice is provided by Contractor and identifies no Non-Conformities, the State will have up to fifteen (15) Business Days to use the Software in the Hosting Environment and determine, in the exercise of its sole discretion, whether it is satisfied that the Software contains no Non-Conformities, on the completion of which the State will, as appropriate:

(i) notify Contractor in writing of Non-Conformities the State has observed in the Software and of the State's non-acceptance thereof, whereupon the parties' rights, remedies and obligations will be as set forth in **Section 13.3** and **Section 13.4**; or

(ii) provide Contractor with a written notice of its Acceptance of such Software, which must be signed by the State's Business Owner and Project Manager.

13.3 Failure of Acceptance Tests. If Acceptance Tests identify any Non-Conformities, Contractor, at Contractor's sole cost and expense, will remedy all such Non-Conformities and re-deliver the Software, in accordance with the requirements set forth in the Statement of Work. Redelivery will occur as promptly as commercially possible and, in any case, within thirty (30) Business Days following, as applicable, Contractor's:

(a) completion of such Acceptance Tests, in the case of Acceptance Tests conducted by Contractor; or

(b) receipt of the State's notice under **Section 13.1(a)** or **Section 13.2(c)(i)**, identifying any Non-Conformities.

13.4 Repeated Failure of Acceptance Tests. If Acceptance Tests identify any Non-Conformity in the Software after a second or subsequent delivery of the Software, or Contractor fails to re-deliver the Software on a timely basis, the State may, in its sole discretion, by written notice to Contractor:

(a) continue the process set forth in this **Section 13**;

(b) accept the Software as a nonconforming deliverable, propose a Change Request proposing the Fees for such Software to be reduced equitably to reflect the value of the Software as received relative to the value of the Software had it conformed; or

(c) deem the failure to be a non-curable material breach of this Contract and the Statement of Work and terminate this Contract for cause in accordance with **Section 24.1**.

13.5 Acceptance. Acceptance ("**Acceptance**") of the Software (subject, where applicable, to the State's right to Integration Testing) will occur on the date that is the earliest of the State's delivery of a notice accepting the Software under **Section 13.2(b)**, or **Section 13.2(c)(ii)**.

14. Training. Contractor shall provide training on all uses of the Software permitted hereunder in accordance with the times, locations and other terms set forth in the Statement of Work. Upon the State's request, Contractor shall timely provide training for additional Authorized Users or other additional training on all uses of the Software for which the State requests such training, at such reasonable times and locations and pursuant to such rates and other terms as are set forth in the Pricing Schedule.

15. Maintenance Releases; New Versions

15.1 Maintenance Releases. Provided that the State is current on its Support Services Fees, during the Term, Contractor shall provide the State, at no additional charge, with all Maintenance Releases, each of which will constitute Software and be subject to the terms and conditions of this Contract.

15.2 New Versions. Provided that the State is current on its Support Services Fees, during the Term, Contractor shall provide the State, at no additional charge, with all New Versions, each of which will constitute Software and be subject to the terms and conditions of this Contract.

15.3 Installation. Subject to Section 14.4, the Contractor will install maintenance releases in the hosted environment.

15.4 Testing By Contractor. Before delivering and installing the Maintenance Releases and New Versions of the Software, Contractor must:

(a) test the Software to confirm that it is fully operable, meets all applicable Specifications and will function in accordance with the Specifications and Documentation when properly installed in the Operating Environment;

(b) scan the Software using industry standard scanning software and definitions to confirm it is free of Harmful Code; and

(c) remedy any Non-Conformity or Harmful Code identified and retest and rescan the Software.

16. Source Code Escrow

16.1 Escrow Contract. The parties may enter into a separate intellectual property escrow agreement. Such escrow agreement will govern all aspects of Source Code escrow and release.

17. Fees

17.1 License Fee. In consideration of, and as payment in full for, the rights and license to use the Software, Third-Party Software, and any associated Documentation as provided in this Contract and the applicable license agreements, the State shall pay to Contractor the license fees (the "**License Fee**") set forth on the Pricing Schedule, subject to and in accordance with the timetable and other provisions of the Statement of Work and this **Section 17**.

17.2 Implementation Fees. In consideration of, and as payment in full for, Contractor's provision of implementation services as provided in this Contract and the Statement of Work, the State shall pay to Contractor the implementation fees (the "**Implementation Fees**") set forth on the Pricing Schedule, subject to and in accordance with the terms and conditions of this Contract, including the applicable timetable and other provisions of the Statement of Work and this **Section 17**.

17.3 Support Service Fees. In consideration of Contractor providing the Support Services as required under the Service Level Agreement, the State shall pay to Contractor the Support Services fees (the "**Support Service Fees**") set forth in the Pricing Schedule, subject to and in accordance with the terms and conditions of this Contract, including the applicable provisions of the Service Level Agreement and this **Section 17**.

17.4 Firm Pricing/Fee Changes. All Pricing set forth in this Contract is firm and will not be increased, except as otherwise expressly provided in this **Section 17.4**.

(a) The License Fee will not be increased at any time except for the addition of additional licenses, the fees for which licenses will also remain firm in accordance with the Pricing set forth in the Pricing Schedule.

18. Invoices and Payment.

18.1 Invoices. Contractor will invoice the State for Fees in accordance with the requirements set forth in the Statement of Work, including any requirements that condition the rendering of invoices and the payment of Fees upon the successful completion of Milestones. Contractor must submit each invoice in both hard copy and electronic format, via such delivery means and to such address as are specified by the State in the Statement of Work. Each separate invoice must:

(a) clearly identify the Contract to which it relates, in such manner as is required by the State;

(b) list each Fee item separately;

(c) include sufficient detail for each line item to enable the State to satisfy its accounting and charge-back requirements;

(d) for Fees determined on a time and materials basis, report details regarding the number of hours performed during the billing period, the skill or labor category for such Contractor Personnel and the applicable hourly billing rates; and

(e) include such other information as may be required by the State as set forth in the Statement of Work.

18.2 Payment. Invoices are due and payable by the State, in accordance with the State's standard payment procedures as specified in 1984 Public Act no. 279, MCL 17.51, *et seq*., within forty-five (45) calendar days after receipt, provided the State determines that the invoice was properly rendered. Payments under this Contract shall be made through Electronic Funds Transfer (EFT). To the extent

permitted by the State's system enabling vendors to register to receive EFT payments and EFT payments may be made to Contractor using the State's system, Contractor must register with the State at http://www.michigan.gov/cpexpress to receive electronic fund transfer payments. If Contractor is permitted to register and EFT payments may be made to Contract using the State's system, but the Contractor does not register, the State is not liable for failure to provide payment.

18.3 Taxes. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Services or Deliverables purchased under this Contract are for the State's exclusive use.

18.4 Service Availability Credits. Contractor acknowledges and agrees that any credits assessed under the Service Level Agreement: (a) are a reasonable estimate of and compensation for the anticipated or actual harm to the State that may arise from not meeting the Availability Requirement or the Support Service Level Requirements, which would be impossible or very difficult to accurately estimate; and (b) may, at the State's option, be credited or set off against any Fees or other charges payable to Contractor under this Contract or be payable to the State upon demand. Credits may not exceed the total amount of Fees that would be payable for the relevant service period in which the credits are assessed. Further, the State may not assess both Service Availability Credits and Service Level Credits for the same Service Error.

18.5 Payment Disputes. The State may withhold from payment any and all payments and amounts the State disputes in good faith, pending resolution of such dispute, provided that the State:

(a) timely renders all payments and amounts that are not in dispute;

(b) notifies Contractor of the dispute prior to the due date for payment, specifying in such notice:

(i) the amount in dispute; and

(ii) the reason for the dispute set out in sufficient detail to facilitate investigation by Contractor and resolution by the parties;

(c) works with Contractor in good faith to resolve the dispute promptly; and

(d) promptly pays any amount determined to be payable by resolution of the dispute.

Contractor shall not withhold any Services or fail to perform any obligation hereunder by reason of the State's good faith withholding of any payment or amount in accordance with this **Section 18.5** or any dispute arising therefrom.

18.6 Right of Setoff. Without prejudice to any other right or remedy it may have, the State reserves the right to set off at any time any amount owing to it by Contractor against any amount payable by the State to Contractor under this Contract.

19. Intellectual Property Rights

19.1 Ownership Rights in Software

(a) Subject to the rights and licenses granted by Contractor in this Contract and the License Agreement, and the provisions of **Section 19.1(b)**:

(i) Contractor reserves and retains its entire right, title and interest in and to all Intellectual Property Rights in and to the Software, including but not limited to all modifications, improvements, and derivative works based thereon, as well as all new inventions, innovations, discoveries, works of authorship, and other things developed, made and created arising out of and relating to Contractor's activities in furtherance of this Contract; and

(ii) none of the State or Authorized Users acquire any ownership of Intellectual Property Rights in or to the Software, Documentation or any of the other items in 18.1(a)(i) above as a result of this Contract.

(b) As between the State, on the one hand, and Contractor, on the other hand, the State has, reserves and retains, sole and exclusive ownership of all right, title and interest in and to State Data and User Data, including all Intellectual Property Rights arising therefrom or relating thereto.

19.2 Rights in Third-Party Software. Ownership of all Third-Party Software, and all Intellectual Property Rights therein, is and will remain with its respective owners, subject to any express licenses or sublicenses granted to the State under this Contract and the Third-Party Licenses.

19.3 Rights in Open-Source Components. Ownership of all Intellectual Property Rights in Open-Source Components shall remain with the respective owners thereof, subject to the State's rights under the applicable Open-Source Licenses.

19.4 Ownership Rights in API. The State is and will be the sole and exclusive owner of all right, title, and interest in and to all API custom-developed by the Contractor for the State for inter-operability with State internally developed software, including all Intellectual Property Rights in and to the API. In furtherance of the foregoing:

(a) Contractor will create all API as work made for hire as defined in Section 101 of the Copyright Act of 1976; and

(b) to the extent any API or Intellectual Property Rights do not qualify as, or otherwise fails to be, work made for hire, Contractor hereby:

(i) assigns, transfers, and otherwise conveys to the State, irrevocably and in perpetuity, throughout the universe, all right, title, and interest in and to such API, including all Intellectual Property Rights in and to the API; and

(ii) irrevocably waives any and all claims Contractor may now or hereafter have in any jurisdiction to so-called "moral rights" or rights of *droit moral* with respect to the API.

20. State Data.

20.1 Ownership. The State's data ("**State Data**"), which will be treated by Contractor as State Confidential Information, includes: (a) User Data; and (b) any other data collected, used, processed, stored, or generated by the State in connection with the Services, including but not limited to (i) personally identifiable information ("**PII**") collected, used, processed, stored, or generated as the result of the Services, including, without limitation, any information that identifies an individual, such as an individual's social security number or other government-issued identification number, date of birth, address, telephone number, biometric data, mother's maiden name, email address, credit card information, or an individual's name in combination with any other of the elements here listed; and (ii) personal health information ("**PHI**") collected, used, processed, stored, or generated as the result of the Services, which is defined under the Health Insurance Portability and Accountability Act ("**HIPAA**") and its related rules and regulations. State Data is and will remain the sole and exclusive property of the State and all right, title, and interest in the same is reserved by the State. This **Section 20.1** survives termination or expiration of this Contract.

20.2 Contractor Use of State Data. Contractor is provided a limited license to State Data for the sole and exclusive purpose of providing the Services, including a license to collect, process, store, generate, and display State Data only to the extent necessary in the provision of the Services. Contractor must: (a) keep and maintain State Data in strict confidence, using such degree of care as is appropriate and consistent with its obligations as further described in this Contract and applicable law to avoid unauthorized access, use, disclosure, or loss; (b) use and disclose State Data solely and exclusively for the purpose of providing the Services, such use and disclosure being in accordance with this Contract, the Statement of Work, and applicable law; and (c) not use, sell, rent, transfer, distribute, or otherwise disclose or make available State Data for Contractor's own purposes or for the benefit of anyone other than the State without the State's prior written consent. This limited license includes the right of Contractor to store State Data in a third party owned and controlled hosted environment (i.e., that is, the cloud) and the transmission of the State Data over third party communication lines. This **Section 20.2** survives termination or expiration of this Contract.

20.3 Data Retention. Specific data retention requirements for the State will be set forth in the Statement of Work.

20.4 Discovery. Contractor shall immediately notify the State upon receipt of any requests which in any way might reasonably require access to State Data or the State's use of the Software. Contractor shall notify the State by the fastest means available and also in writing. In no event shall Contractor provide such notification more than twenty-four (24) hours after Contractor receives the request. Contractor shall not respond to subpoenas, service of process, FOIA requests, and other legal requests related to State Data without first notifying the State and obtaining the State's prior approval of Contractor's proposed responses. Contractor agrees to provide its completed responses to the State with adequate time for review, revision and approval

20.5 Loss or Compromise of Data. In the event of any act, error or omission, negligence, misconduct, or breach on the part of Contractor that compromises or is suspected to compromise the security, confidentiality, or integrity of State Data or the physical, technical, administrative, or organizational safeguards put in place by Contractor that relate to the protection of the security, confidentiality, or integrity of State Data, Contractor must, as applicable: (a) notify the State as soon as practicable but no later than twenty-four (24) hours of becoming aware of such occurrence; (b) cooperate with the State in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by the State; (c) in the case of PII or PHI, at the State's sole election, (i) with approval and assistance from the State, notify the affected individuals who comprise the PII or PHI as soon as practicable but no later than is required to comply with applicable law, or, in the absence of any legally required notification period, within five (5) calendar days of the occurrence; or (ii) reimburse the State for any costs in notifying the affected individuals; (d) in the case of PII, provide third-party credit and identity monitoring services to each of the affected individuals who comprise the PII for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than twelve (12) months following the date of notification to such individuals; (e) perform or take any other actions required to comply with applicable law as a result of the occurrence; (f) pay for any costs associated with the occurrence, including but not limited to any costs incurred by the State in investigating and resolving the occurrence, including reasonable attorney's fees associated with such investigation and resolution; (g) without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the occurrence; (h) be responsible for recreating lost State Data in the manner and on the schedule set by the State without charge to the State; and (i) provide to the State a detailed plan within ten (10) calendar days of the occurrence describing the measures Contractor will undertake to prevent a future occurrence. Notification to affected individuals, as described above, must comply with applicable law, be written in plain language, not be tangentially used for any solicitation purposes, and contain, at a minimum: name and contact information of Contractor's representative; a description of the nature of the loss; a list of the types of data involved; the known or approximate date of the loss; how such loss may affect the affected individual; what steps Contractor has taken to protect the affected individual; what steps the affected individual can take to protect himself or herself; contact information for major credit card reporting agencies; and, information regarding the credit and identity monitoring services to be provided by Contractor. The State will have the option to review and approve any notification sent to affected individuals prior to its delivery. Notification to any other party, including but not limited to public media outlets, must be reviewed and approved by the State in writing prior to its dissemination. This **Section** survives termination or expiration of this Contract.

21. Confidential Information. Each party acknowledges that it may be exposed to or acquire communication or data of the other party that is confidential in nature and is not intended to be disclosed to third parties. This **Section 21** survives termination or expiration of this Contract.

21.1 Meaning of Confidential Information. The term "**Confidential Information**" means all information and documentation of a party that: (a) has been marked "confidential" or with words of similar

meaning, at the time of disclosure by such party; (b) if disclosed orally or not marked “confidential” or with words of similar meaning, was subsequently summarized in writing by the disclosing party and marked “confidential” or with words of similar meaning; or, (c) should reasonably be recognized as confidential information of the disclosing party. The term “Confidential Information” does not include any information or documentation that was or is: (a) in the possession of the State and subject to disclosure under the Michigan Freedom of Information Act (FOIA); (b) already in the possession of the receiving party without an obligation of confidentiality; (c) developed independently by the receiving party, as demonstrated by the receiving party, without violating the disclosing party’s proprietary rights; (d) obtained from a source other than the disclosing party without an obligation of confidentiality; or, (e) publicly available when received, or thereafter became publicly available (other than through any unauthorized disclosure by, through, or on behalf of, the receiving party). Notwithstanding the above, in all cases and for all matters, State Data is deemed to be Confidential Information.

21.2 Obligation of Confidentiality. The parties agree to hold all Confidential Information in strict confidence and not to copy, reproduce, sell, transfer, or otherwise dispose of, give or disclose such Confidential Information to third parties other than employees, agents, or subcontractors of a party who have a need to know in connection with this Contract or to use such Confidential Information for any purposes whatsoever other than the performance of this Contract. The parties agree to advise and require their respective employees, agents, and subcontractors of their obligations to keep all Confidential Information confidential. Disclosure to the Contractor’s subcontractor is permissible where: (a) the subcontractor is a Permitted Subcontractor; (b) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the Permitted Subcontractor's responsibilities; and (c) Contractor obligates the Permitted Subcontractor in a written contract to maintain the State’s Confidential Information in confidence. At the State’s request, any of the Contractor’s Representatives may be required to execute a separate agreement to be bound by the provisions of this **Section 21.2**.

21.3 Cooperation to Prevent Disclosure of Confidential Information. Each party must use its best efforts to assist the other party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the foregoing, each party must advise the other party immediately in the event either party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Contract. Each party will cooperate with the other party in seeking injunctive or other equitable relief against any such person.

21.4 Remedies for Breach of Obligation of Confidentiality. Each party acknowledges that breach of its obligation of confidentiality may give rise to irreparable injury to the other party, which damage may be inadequately compensable in the form of monetary damages. Accordingly, a party may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies which may be available, to include, in the case of the State, at the sole election of the State, the immediate termination, without liability to the State, of this Contract or any Statement of Work corresponding to the breach or threatened breach.

21.5 Surrender of Confidential Information upon Termination. Upon termination or expiration of this Contract or a Statement of Work, in whole or in part, each party must, within ten (10) Business Days from the date of termination, return to the other party any and all Confidential Information received from the

other party, or created or received by a party on behalf of the other party, which are in such party's possession, custody, or control. If Contractor or the State determine that the return of any Confidential Information is not feasible, such party must destroy the Confidential Information and certify the same in writing within ten (10) Business Days from the date of termination to the other party.

22. HIPAA Compliance. The State and Contractor must comply with all applicable obligations under HIPAA and its accompanying regulations, including but not limited to entering into a business associate agreement, if applicable and reasonably necessary to keep the State and Contractor in compliance with HIPAA.

23. ADA Compliance. The State is required to comply with the Americans with Disabilities Act of 1990 (ADA), and has adopted a formal policy regarding accessibility requirements for websites and software applications. Contractor's Service Software must comply, where relevant, with level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0.

24. Termination, Expiration, Transition. The State may terminate this Contract, the Support Services, or any Statement of Work, in accordance with the following:

24.1 Termination for Cause. In addition to any right of termination set forth elsewhere in this Contract:

(a) The State may terminate this Contract for cause, in whole or in part, if Contractor,: (i) endangers the value, integrity, or security of State Systems, State Data, or the State's facilities or personnel; (ii) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor; or (iii) breaches any of its material duties or obligations under this Contract; and Contractor fails to cure any of the aforementioned material breach events within thirty (30) days of the date the State provided Contractor with written notice specifically describing the applicable event . Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.

(b) If Contractor fails to cure its material breach within the cure period and the State terminates this Contract under this **Section 24.1**, the State will issue a termination notice specifying whether Contractor must: (a) cease performance immediately, or (b) continue to perform for a specified period. If it is later determined that Contractor was not in breach of this Contract, the termination will be deemed to have been a termination for convenience, effective as of the same date, and the rights and obligations of the parties will be limited to those provided in **Section 24.2**.

(c) Where the Contract was terminated by the State for an uncured material breach, the State will only pay for amounts due to Contractor for Services accepted by the State on or before the date of termination, subject to the State's right to set off any amounts owed by the Contractor for the State's reasonable costs in terminating this Contract. If the State itself is not alleged to be in breach of this Contract, then: (a) Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination, including any prepaid Support Services Fees; and (b) Contractor must pay all reasonable costs incurred by the State in terminating this Contract for cause, including

administrative costs, reasonable attorneys' fees, court costs, and any reasonable out of pocket costs the State incurs to procure the Services from other sources. The State shall undertake all reasonable efforts under applicable law to mitigate its damages.

24.2 Termination for Convenience. The State may immediately terminate this Contract in whole or in part, without penalty and for any reason, including but not limited to, appropriation or budget shortfalls. The termination notice will specify whether Contractor must: (a) cease performance immediately, or (b) continue to perform in accordance with **Section 24.3**. If the State terminates this Contract for convenience, the State will pay all reasonable costs for services provided prior to termination. Notwithstanding the foregoing, if the termination is for non-appropriation, the State will pay for all reasonable costs to the extent funds are available.

24.3 Transition Responsibilities. Upon termination or expiration of this Contract for any reason, Contractor must, for a period of time specified by the State (not to exceed 90 calendar days; the "**Transition Period**"), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Contract to continue without interruption or adverse effect, and to facilitate the orderly transfer of the Services to the State or its designees. Such transition assistance may include but is not limited to: (a) continuing to perform the Services at the established Contract rates and payment terms; (b) taking all reasonable and necessary measures (which does not include the provision or transfer of the Contractor's Software) to transition performance of the work, including all applicable Services to the State or the State's designee; (c) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, or return to the State all State Data, it being acknowledged and agreed to by Contractor that return of State Data will be in the usable format specified by the State in this Contract and without any conditions or contingencies whatsoever (including but not limited to the payment of any fees to Contractor – it being the responsibility of the subsequent contractor to convert the format the State Data specified in this Contract to any different format); and (d) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts (collectively, the "**Transition Responsibilities**"). The Term of this Contract is automatically extended through the end of the Transition Period.

24.4 Survival. This **Section 24** survives termination or expiration of this Contract.

25. Stop Work Order. The State may, at any time, order the Services of Contractor fully or partially stopped for its own convenience for up to ninety (90) calendar days at no additional cost to the State. The State will provide Contractor a written notice detailing such suspension (a "**Stop Work Order**"). Contractor must comply with the Stop Work Order upon receipt. Within 90 days, or any longer period agreed to by Contractor, the State will either: (a) issue a notice authorizing Contractor to resume work, or (b) terminate this Contract as provided in Section 24. The State will not pay for any Services, Contractor's lost profits, or any additional compensation during a stop work period.

26. Contractor Representations and Warranties.

26.1 Authority. Contractor represents and warrants to the State that:

(a) It is duly organized, validly existing, and in good standing as a corporation or other entity as represented under this Contract under the laws and regulations of its jurisdiction of incorporation, organization, or chartering;

(b) It has the full right, power, and authority to enter into this Contract, to grant the rights and licenses granted under this Contract, and to perform its contractual obligations;

(c) The execution of this Contract by its Representative has been duly authorized by all necessary organizational action; and

(d) When executed and delivered by Contractor, this Contract will constitute the legal, valid, and binding obligation of Contractor, enforceable against Contractor, its legal successors in interest and permitted assignees in accordance with its terms.

26.2 Bid Response. Contractor represents and warrants to the State that:

(a) The prices proposed by Contractor were arrived at independently, without consultation, communication, or agreement with any other bidder for the purpose of restricting competition; the prices quoted were not knowingly disclosed by Contractor to any other bidder to the RFP; and no attempt was made by Contractor to induce any other Person to submit or not submit a proposal for the purpose of restricting competition;

(b) All written information furnished to the State by or for Contractor in connection with this Contract, including Contractor's Bid Response, is true, accurate, and complete, and contains no untrue statement of material fact or omits any material fact necessary to make the information not misleading;

(c) Contractor is not in material default or breach of any other contract or agreement that it may have with the State or any of its departments, commissions, boards, or agencies. Contractor further represents and warrants that it has not been a party to any contract with the State or any of its departments that was terminated by the State within the previous five (5) years for the reason that Contractor failed to perform or otherwise breached an obligation of the contract; and

(d) If any of the certifications, representations, or disclosures made in Contractor's Bid Response change after contract award, the Contractor is required to report those changes immediately to the Contract Administrator.

26.3 Software Representations and Warranties. Contractor further represents and warrants to the State that:

(a) it is the legal and beneficial owner of the entire right, title and interest in and to the Software, including all Intellectual Property Rights relating thereto;

(b) it has, and throughout the license term, will retain the unconditional and irrevocable right, power and authority to grant and perform the license hereunder;

(c) the Software, and the State's use thereof, is and throughout the license term will be free and clear of all encumbrances, liens and security interests of any kind;

(d) neither its grant of the license, nor its performance under this Contract does or to its knowledge will at any time:

(i) conflict with or violate any applicable Law;

(ii) require the consent, approval or authorization of any governmental or regulatory authority or other third party; or

(iii) require the provision of any payment or other consideration to any third party;

(e) when used by the State or any Authorized User in accordance with this Contract and the Documentation, the Software or Documentation as delivered or installed by Contractor does not or will not knowingly:

(i) infringe, misappropriate or otherwise violate any Intellectual Property Right or other right of any third party; or

(ii) fail to comply with any applicable Law;

(f) as provided by Contractor, the Software does not or will not at any time during the license term contain any:

(i) Harmful Code; or

(ii) Open-Source Components or operate in such a way that it is developed or compiled with or linked to any Open-Source Components, other than Open-Source Components specifically described in the Statement of Work.

(g) all Documentation is and will be complete and accurate in all material respects when provided to the State such that at no time during the license term will the Software have any material undocumented feature; and

(h) it will perform all Services in a timely, skillful, professional and workmanlike manner in accordance with commercially reasonable industry standards and practices for similar services, using personnel with the requisite skill, experience and qualifications, and will devote adequate resources to meet its obligations under this Contract.

(i) when used in the Hosting Environment (or any successor thereto) in accordance with the Documentation, all Software as provided by Contractor, will be fully operable, meet all applicable specifications, and function in all material respects, in conformity with this Contract and the Documentation; and

(j) no Maintenance Release or New Version, when properly installed by Contractor in accordance with this Contract, will have a material adverse effect on the functionality or operability of the Software.

26.4 Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THIS AGREEMENT, CONTRACTOR HEREBY DISCLAIMS ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THIS CONTRACT.

27. Indemnification

27.1 General Indemnification. Contractor must defend, indemnify and hold the State, its departments, divisions, agencies, offices, commissions, officers, and employees harmless, without limitation, from and against any and all third party actions, claims, losses, liabilities, damages, costs, attorney fees, and expenses (including reasonable outside attorney's fees incurred to establish the right to indemnification), arising out of or relating to: (a) any breach by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable) of any of the promises, agreements, representations, warranties, or insurance requirements contained in this Contract; (b) any infringement, misappropriation, or other violation of any Intellectual Property Right or other right of any Third Party; and (c) any bodily injury, death, or damage to real or tangible personal property occurring wholly or in part due to action or inaction by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable).

27.2 Indemnification Procedure. The State will promptly notify Contractor in writing upon receipt of any third party action or claim if defense and indemnification is sought; however, failure to do so will not relieve Contractor, except to the extent that Contractor is materially prejudiced. Contractor must, to the reasonable satisfaction of the State, demonstrate its financial ability to carry out these obligations. The State is entitled to: (i) regular updates on proceeding status; (ii) participate in the defense of the proceeding; (iii) employ its own counsel at its own expense; and to (iv) waive its right to defense and indemnification by retaining control of the defense, at its own cost and expense, if the State deems necessary. Contractor will not, without the State's prior written consent (not to be unreasonably withheld), settle, compromise, or consent to the entry of any judgment in or otherwise seek to terminate any claim, action, or proceeding. Contractor has no duty to defend or indemnify the State if the State settles the third party action or claim without obtaining Contractor's prior express written approval from Contractor's Chief Executive Officer and General Counsel. Any litigation activity on behalf of the State or any of its subdivisions, under this **Section 27**, must be coordinated with the Department of Attorney General. An attorney designated to represent the State may not do so until approved by the Michigan Attorney General and appointed as a Special Assistant Attorney General.

27.3 Infringement Remedies.

(a) The remedies set forth in this **Section 27.3** are in addition to, and not in lieu of, all other remedies that may be available to the State under this Contract or otherwise, including the State's right to be indemnified for such actions.

(b) If any Software or any component thereof, other than State Materials, is found to be infringing or if any use of any Software or any component thereof is enjoined, threatened to be enjoined or otherwise the subject of an infringement claim, Contractor must, at Contractor's sole cost and expense:

(i) procure for the State the right to continue to use such Software or component thereof to the full extent contemplated by this Contract; or

(ii) modify or replace the materials that infringe or are alleged to infringe ("**Allegedly Infringing Materials**") to make the Software and all of its components non-infringing while providing fully equivalent features and functionality.

(c) If neither of the foregoing is possible notwithstanding Contractor's best efforts, then Contractor may direct the State to cease any use of any materials that have been enjoined or finally adjudicated as infringing, provided that Contractor will:

(i) refund to the State all amounts paid by the State in respect of such Allegedly Infringing Materials and any other aspects of the Software provided under the Statement of Work for the Allegedly Infringing Materials that the State cannot reasonably use as intended under this Contract; and

(ii) in any case, at its sole cost and expense, secure the right for the State to continue using the Allegedly Infringing Materials for a transition period of up to six (6) months to allow the State to replace the affected features of the Software without disruption.

(d) If Contractor directs the State to cease using any Software under **subsection (c)**, the State may terminate this Contract for cause under **Section 24.1**.

(e) Contractor will have no liability for any claim of infringement to the extent resulting from:

(i) Contractor's compliance with any designs, specifications, or instructions of the State; or

(ii) modification of the Software by the State without the prior knowledge and approval of Contractor; or

(iii) combination of the Software by the State with any other product, service or item not provided by Contractor; or

(iv) the State's continued use of the Software after Contractor notified the State and offered the State replacement non-infringing software;

unless the claim arose against the Software independently of any of the above specified actions.

28. Damages Disclaimers and Limitations.

28.1 Disclaimer of Damages. NEITHER PARTY WILL BE LIABLE TO THE OTHER, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT FOR CONSEQUENTIAL, INCIDENTAL, INDIRECT, OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST PROFITS AND LOST BUSINESS OPPORTUNITIES.

28.2 Limitation of Liability. IN NO EVENT WILL EITHER PARTY'S AGGREGATE LIABILITY TO THE OTHER UNDER THIS CONTRACT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT, EXCEED THE AGGREGATE AMOUNT OF FEES SPECIFIED IN THE STATEMENT OF WORK. NOTWITHSTANDING THE FOREGOING, SUCH LIMITATION OF LIABILITY WILL NOT APPLY TO (I) EITHER PARTY'S BREACH OF ITS CONFIDENTIALITY OBLIGATIONS, (II) CONTRACTOR'S INDEMNIFICATION OBLIGATIONS, OR (III) CONTRACTOR'S OBLIGATIONS UNDER SECTION 20.5.

29. Records Maintenance, Inspection, Examination, and Audit.

29.1 Right of Audit. The State or its designee may audit Contractor to verify compliance with this Contract. Contractor must retain, and provide to the State or its designee and the auditor general upon request, all financial and accounting records related to this Contract through the Term of this Contract and for four (4) years after the latter of termination, expiration, or final payment under this Contract or any extension ("**Financial Audit Period**"). If an audit, litigation, or other action involving the records is initiated before the end of the Financial Audit Period, Contractor must retain the records until all issues are resolved.

29.2 Right of Inspection. Within ten (10) calendar days of providing notice, the State and its authorized representatives or designees have the right to enter and inspect Contractor's premises or any other places where Services are being performed, and examine, copy, and audit all records related to this Contract. Contractor must cooperate and provide reasonable assistance. If financial errors are revealed, the amount in error must be reflected as a credit or debit on subsequent invoices until the amount is paid or refunded. Any remaining balance at the end of this Contract must be paid or refunded within forty-five (45) calendar days.

29.3 Application. This **Section 29** applies to Contractor, any Affiliate, and any Permitted Subcontractor that performs Services in connection with this Contract, along with such parties' legal successors in interest and permitted assignees.

30. Insurance

30.1 Required Coverage.

(a) **Insurance Requirements.** Contractor must maintain the insurances identified below and is responsible for all deductibles. All required insurance must: (a) protect the State from claims that may arise out of, are alleged to arise out of, or result from Contractor's or a subcontractor's performance; (b) be primary and non-contributing to any comparable liability insurance (including self-insurance) carried by the State; and (c) be provided by an company with an A.M. Best rating of "A" or better and a financial size of VII or better.

Insurance Type	Additional Requirements
Commercial General Liability Insurance	
Minimal Limits: $1,000,000 Each Occurrence Limit $1,000,000 Personal & Advertising Injury Limit $2,000,000 General Aggregate Limit $2,000,000 Products/Completed Operations Deductible Maximum: $50,000 Each Occurrence	Contractor must have their policy endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as additional insureds using endorsement CG 20 10 11 85, or both CG 2010 07 04 and CG 2037 07 0.
Umbrella or Excess Liability Insurance	
Minimal Limits: $5,000,000 General Aggregate	Contractor must have their policy endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as additional insureds.
Workers' Compensation Insurance	
Minimal Limits: Coverage according to applicable laws governing work activities.	Waiver of subrogation, except where waiver is prohibited by law.
Employers Liability Insurance	
Minimal Limits: $500,000 Each Accident $500,000 Each Employee by Disease	

$500,000 Aggregate Disease.	
Privacy and Security Liability (Cyber Liability) Insurance	
Minimal Limits: $2,000,000 Each Occurrence $2,000,000 Annual Aggregate	Contractor must have their policy: (1) endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as additional insureds; and (2) cover information security and privacy liability, privacy notification costs, regulatory defense and penalties, and website media content liability.

(b) The minimum limits are not intended, and may not be construed to limit any liability or indemnity of Contractor to any indemnified party or other persons.

(c) If any of the required policies provide claim-made coverage, the Contractor must: (a) provide coverage with a retroactive date before the effective date of the contract or the beginning of contract work; (b) maintain coverage and provide evidence of coverage for at least three (3) years after completion of the contract of work; and (c) if coverage is canceled or not renewed, and not replaced with another claims-made policy form with a retroactive date prior to the contract effective date, Contractor must purchase extended reporting coverage for a minimum of three (3) years after completion of work.

(d) Contractor must: (a) provide insurance certificates to the Contract Administrator, containing the agreement or purchase order number, at Contract formation and within 20 calendar days of the expiration date of the applicable policies; (b) require that subcontractors maintain the required insurances contained in this Section; (c) notify the Contract Administrator within 5 business days if any insurance is cancelled; and (d) waive all rights against the State for damages covered by insurance. Failure to maintain the required insurance does not limit this waiver.

30.2 Non-waiver. This **Section 30** is not intended to and is not be construed in any manner as waiving, restricting or limiting the liability of either party for any obligations under this Contract (including any provisions hereof requiring Contractor to indemnify, defend and hold harmless the State).

31. Dispute Resolution.

31.1 Unless otherwise specified in the Statement of Work, the parties will endeavor to resolve any Contract dispute in accordance with **Section 31** (the "**Dispute Resolution Procedure**"). The initiating party will reduce its description of the dispute to writing (including all supporting documentation) and deliver it to the responding party's Project Manager. The responding party's Project Manager must respond in writing within five (5) Business Days. The initiating party has five (5) Business Days to review

the response. If after such review resolution cannot be reached, both parties will have an additional five (5) Business Days to negotiate in good faith to resolve the dispute. If the dispute cannot be resolved within a total of fifteen (15) Business Days, the parties must submit the dispute to the parties' Contract Administrators. The parties will continue performing while a dispute is being resolved, unless the dispute precludes performance. A dispute involving payment does not preclude performance.

31.2 Litigation to resolve the dispute will not be instituted until after the dispute has been elevated to the parties' Contract Administrators, and either Contract Administrator concludes that resolution is unlikely, or fails to respond within fifteen (15) Business Days. The parties are not prohibited from instituting formal proceedings: (a) to avoid the expiration of statute of limitations period; (b) to preserve a superior position with respect to creditors; or (c) where a party makes a determination that a temporary restraining order or other injunctive relief is the only adequate remedy. This **Section 31** does not limit the State's right to terminate this Contract.

32. General Provisions

32.1 Force Majeure.

(a) Force Majeure Events. Subject to **Subsection (b)** below, neither party will be liable or responsible to the other party, or be deemed to have defaulted under or breached this Contract, for any failure or delay in fulfilling or performing any term hereof, when and to the extent such failure or delay is caused by: acts of God, flood, fire or explosion, war, terrorism, invasion, riot or other civil unrest, embargoes or blockades in effect on or after the date of this Contract, national or regional emergency, or any passage of law or governmental order, rule, regulation or direction, or any action taken by a governmental or public authority, including imposing an embargo, export or import restriction, quota or other restriction or prohibition (each of the foregoing, a "**Force Majeure**"), in each case provided that: (a) such event is outside the reasonable control of the affected party; (b) the affected party gives prompt written notice to the other party, stating the period of time the occurrence is expected to continue; (c) the affected party uses diligent efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

(b) State Performance; Termination. In the event of a Force Majeure Event affecting Contractor's performance under this Contract, the State may suspend its performance hereunder until such time as Contractor resumes performance. The State may terminate this Contract by written notice to Contractor if a Force Majeure Event affecting Contractor's performance hereunder continues substantially uninterrupted for a period of five (5) Business Days or more. Unless the State terminates this Contract pursuant to the preceding sentence, any date specifically designated for Contractor's performance under this Contract will automatically be extended for a period up to the duration of the Force Majeure Event. Notwithstanding the foregoing, Contractor will be excused of its obligations under Service Level Agreement if a Force Majeure Event simultaneously and materially impairs the ability of the Contractor to deliver the Hosted Services from all of its operating and backup sites.

32.2 Further Assurances. Each party will, upon the reasonable request of the other party, execute such documents to provide further assurances and perform such acts as may be necessary to give full effect to the terms of this Contract.

32.3 Relationship of the Parties. The relationship between the parties is that of independent contractors. Nothing contained in this Contract is to be construed as creating any agency, partnership, joint venture or other form of joint enterprise, employment or fiduciary relationship between the parties, and neither party has authority to contract for or bind the other party in any manner whatsoever.

32.4 Media Releases. News releases (including promotional literature and commercial advertisements) pertaining to this Contract or project to which it relates must not be made without the prior written approval of the State, and then only in accordance with the explicit written instructions of the State.

32.5 Notices. All notices, requests, consents, claims, demands, waivers and other communications under this Contract must be in writing and addressed to the parties as follows (or as otherwise specified by a party in a notice given in accordance with this **Section 32.5**):

If to Contractor:	2255 St Laurent Blvd., Suite 206	
	Ottawa, ON K1G 4K3 CANADA	
	Email:	jocelyn.tremblay@stacsdna.com
	Attention:	Jocelyn Tremblay
If to State:	525 W. Allegan, 1st Floor	
	Lansing, MI 48909	
	Email:	taylort27@michigan.gov
	Attention:	Timothy Taylor

Notices sent in accordance with this **Section 32.5** will be deemed effectively given: (a) when received, if delivered by hand (with written confirmation of receipt); (b) when received, if sent by a nationally recognized overnight courier (receipt requested); (c) on the date sent by e-mail (with confirmation of transmission), if sent during normal business hours of the recipient, and on the next Business Day, if sent after normal business hours of the recipient; or (d) on the fifth (5th) day after the date mailed, by certified or registered mail, return receipt requested, postage prepaid.

32.6 Headings. The headings in this Contract are for reference only and do not affect the interpretation of this Contract.

32.7 Assignment. Contractor may not assign or otherwise transfer any of its rights, or delegate or otherwise transfer any of its obligations or performance, under this Contract, in each case whether

voluntarily, involuntarily, by operation of law or otherwise, without the State's prior written consent. The State has the right to terminate this Contract in its entirety or any Services or Statements of Work hereunder, pursuant to **Section 24.1**, if Contractor delegates or otherwise transfers any of its obligations or performance hereunder, whether voluntarily, involuntarily, by operation of law or otherwise, and no such delegation or other transfer will relieve Contractor of any of such obligations or performance. For purposes of the preceding sentence, and without limiting its generality, any merger, consolidation or reorganization involving Contractor (regardless of whether Contractor is a surviving or disappearing entity) will be deemed to be a transfer of rights, obligations, or performance under this Contract for which the State's prior written consent is required. Any purported assignment, delegation, or transfer in violation of this **Section 32.7** is void.

32.8 No Third-party Beneficiaries. This Contract is for the sole benefit of the parties and their respective successors and permitted assigns. Nothing herein, express or implied, is intended to or will confer on any other person or entity any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this Contract.

32.9 Amendment and Modification; Waiver. No amendment to or modification of this Contract is effective unless it is in writing, identified as an amendment to this Contract and signed by both parties Contract Administrator or higher ranking officer. Further, certain amendments to this Contract may require State Administrative Board Approval. No waiver by any party of any of the provisions of this Contract will be effective unless explicitly set forth in writing and signed by the party so waiving. Except as otherwise set forth in this Contract, no failure to exercise, or delay in exercising, any right, remedy, power, or privilege arising from this Contract will operate or be construed as a waiver. Nor will any single or partial exercise of any right, remedy, power or privilege under this Contract preclude the exercise of any other right, remedy, power or privilege.

32.10 Severability. If any term or provision of this Contract is invalid, illegal or unenforceable in any jurisdiction, such invalidity, illegality or unenforceability will not affect any other term or provision of this Contract or invalidate or render unenforceable such term or provision in any other jurisdiction. Upon such determination that any term or other provision is invalid, illegal or unenforceable, the parties hereto will negotiate in good faith to modify this Contract so as to effect the original intent of the parties as closely as possible in a mutually acceptable manner in order that the transactions contemplated hereby be consummated as originally contemplated to the greatest extent possible.

32.11 Governing Law. This Contract is governed, construed, and enforced in accordance with Michigan law, excluding choice-of-law principles, and all claims relating to or arising out of this Contract are governed by Michigan law, excluding choice-of-law principles. Any dispute arising from this Contract must be resolved in the Michigan Court of Claims. Complaints against the State must be initiated in Ingham County, Michigan. Contractor waives any objections, such as lack of personal jurisdiction or forum non conveniens. Contractor must appoint agents in Michigan to receive service of process.

32.12 Equitable Relief. Each party to this Contract acknowledges and agrees that (a) a breach or threatened breach by such party of any of its obligations under this Contract may give rise to irreparable harm to the other party for which monetary damages would not be an adequate remedy and (b) in the

event of a breach or a threatened breach by such party of any such obligations, the other party hereto is, in addition to any and all other rights and remedies that may be available to such party at law, at equity or otherwise in respect of such breach, entitled to seek equitable relief, including a temporary restraining order, an injunction, specific performance and any other relief that may be available from a court of competent jurisdiction, without any requirement to post a bond or other security, and without any requirement to prove actual damages or that monetary damages will not afford an adequate remedy. Each party to this Contract agrees that such party will not oppose or otherwise challenge the appropriateness of equitable relief or the entry by a court of competent jurisdiction of an order granting equitable relief, in either case, consistent with the terms of this **Section 32.12**.

32.13 Nondiscrimination. Under the Elliott-Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, *et seq*., and the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, et seq., Contractor and its Permitted Subcontractors agree not to discriminate against an employee or applicant for employment with respect to hire, tenure, terms, conditions, or privileges of employment, or a matter directly or indirectly related to employment, because of race, color, religion, national origin, age, sex, height, weight, marital status, or mental or physical disability. Breach of this covenant is a material breach of this Contract.

32.14 Unfair Labor Practice. Under MCL 423.324, the State may void any Contract with a Contractor or Permitted Subcontractor who appears on the Unfair Labor Practice register compiled under MCL 423.322.

32.15 Counterparts. This Contract may be executed in counterparts, each of which will be deemed an original, but all of which together are deemed to be one and the same agreement and will become effective and binding upon the parties as of the Effective Date at such time as all the signatories hereto have signed a counterpart of this Contract. A signed copy of this Contract delivered by facsimile, e-mail or other means of electronic transmission (to which a signed copy is attached) is deemed to have the same legal effect as delivery of an original signed copy of this Contract.

32.16 Effect of Contractor Bankruptcy. All rights and licenses granted by Contractor under this Contract are and will be deemed to be rights and licenses to "intellectual property," and all Software and Deliverables are and will be deemed to be "embodiments" of "intellectual property," for purposes of, and as such terms are used in and interpreted under, Section 365(n) of the United States Bankruptcy Code (the "**Code**"). If Contractor or its estate becomes subject to any bankruptcy or similar proceeding, the State retains and has the right to fully exercise all rights, licenses, elections, and protections under this Contract, the Code and all other applicable bankruptcy, insolvency, and similar Laws with respect to all Software and other Deliverables. Without limiting the generality of the foregoing, Contractor acknowledges and agrees that, if Contractor or its estate shall become subject to any bankruptcy or similar proceeding:

(a) all rights and licenses granted to the State under this Contract will continue subject to the terms and conditions of this Contract, and will not be affected, even by Contractor's rejection of this Contract; and

(b) the State will be entitled to a complete duplicate of (or complete access to, as appropriate) all such intellectual property and embodiments of intellectual property comprising or relating to any Software or other Deliverables, and the same, if not already in the State's possession, will be promptly delivered to the State, unless Contractor elects to and does in fact continue to perform all of its obligations under this Contract. In no event, however, will the State's license rights to the Software be expanded from the limited license to use the Software as expressly provided herein.

32.17 Compliance with Laws. Contractor and its Representatives must comply with all applicable laws in connection with this Contract.

32.18 Non-Exclusivity. Nothing contained in this Contract is intended nor is to be construed as creating any requirements contract with Contractor. This Contract does not restrict the State or its agencies from acquiring similar, equal, or like Services from other sources.

32.19 Entire Agreement. This Contract, together with all Schedules, Exhibits, and the Statement of Work constitutes the sole and entire agreement of the parties to this Contract with respect to the subject matter contained herein, and supersedes all prior and contemporaneous understandings and agreements, representations and warranties, both written and oral, with respect to such subject matter. In the event of any inconsistency between the statements made in the body of this Contract, the Schedules, Exhibits, and the Statement of Work, the following order of precedence governs: (a) first, this Contract, excluding its Exhibits and Schedules, and the Statement of Work; and (b) second, the Statement of Work as of the Effective Date; and (c) third, the Exhibits and Schedules to this Contract as of the Effective Date. NO TERMS ON CONTRACTOR'S OR THE STATE'S INVOICES, WEBSITE, BROWSE-WRAP, SHRINK-WRAP, CLICK-WRAP, CLICK-THROUGH OR OTHER NON-NEGOTIATED TERMS AND CONDITIONS PROVIDED WITH ANY OF THE SERVICES, OR DOCUMENTATION HEREUNDER WILL CONSTITUTE A PART OR AMENDMENT OF THIS CONTRACT OR IS BINDING ON THE OTHER PARTY OR ANY AUTHORIZED USER FOR ANY PURPOSE. ALL SUCH OTHER TERMS AND CONDITIONS HAVE NO FORCE AND EFFECT AND ARE DEEMED REJECTED BY THE PARTIES AND THE AUTHORIZED USER, EVEN IF ACCESS TO OR USE OF SUCH SERVICE OR DOCUMENTATION REQUIRES AFFIRMATIVE ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

SCHEDULE A
STATEMENT OF WORK (SOW)

1. DEFINITIONS

For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this Section 1 shall have the respective meanings given to them in the Contract Terms.

Term	Description
ADA	Americans with Disabilities Act of 1990
AES	Advanced Encryption Standard
BAA	Business Associate Agreement
CJIS	Criminal Justice Information Services
DTMB	Department of Technology, Management & Budget
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
HIPAA	Health Insurance Portability and Accountability Act
ICHAT	Internet Criminal History Access Tool
LCMS	Laboratory Case Management Solution
LEA	Law Enforcement Agency
MOD	NIST Minimum Security Controls - Moderate-Impact Baseline
MS	Microsoft
MSP	Michigan State Police
MSP-FSD	Michigan State Police - Forensic Science Division
NCIC	National Crime Information Center
NIST	National Institute of Standards and Technology
PM	Project Manager
PMBoK	Project Management Institute's Book of Knowledge
PMI	Project Management Institute
PMM	Project Management Methodology
Policy Center	Policy Center is the Administrating Agency
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAEK	Sexual Assault Evidence Kit
SAEKs	Sexual Assault Evidence Kits
SAML	Security Assertion Markup Language
SEM	Solutions Engineering Methodology
SLA	Service Level Agreement
SMMS	Social Media Management Software
SOM	State of Michigan
SSAE	Statement on Standards for Attestation Engagements
SSO	Single Sign-on
SUITE	State Unified Information Technology Environment
VPAT	Voluntary Product Accessibility Template
W3C	World Wide Web Consortium
WBS	Work Breakdown Structure
WCAG	Web Content Accessibility Guidelines

2. INTRODUCTION AND PURPOSE

2.1 Introduction

Contractor will implement a centrally-managed cloud-based Sexual Assault Evidence Kits (SAEKs) Solution, referred to as "Solution" or "Track-Kit" to electronically track the status of sexual assault evidence kits from the point of distribution to healthcare providers through the return to law enforcement after the completion of laboratory processing and examination for the entire State of Michigan (referred to as the "State" or "SOM").

The Track-Kit product details are as follows:

Product name:	Track-Kit
Product version:	2
Product release number:	3

The Solution will require limited custom development to meet the requirements defined in this SOW. All software enhancements implemented by the Contractor in the Track-Kit will be in a single codebase. Any and all new features and functions implemented in the Track-Kit will automatically cascade down to all Track-Kit clients. Contractor will ensure that the State stays current with each future Product version and release number of the Solution without any additional cost.

Track-Kit will be hosted in the Contractor's Microsoft Azure Government Cloud environment designed for stringent security and performance requirements as described in Schedule E. Disaster Recovery Plan and Schedule F. Disaster Security Terms. The Contractor's Microsoft Azure Government Cloud will provide and Contractor will support multiple environments: User Acceptance Testing (Staging), Training, and Production. Staging and Training environments must mirror the Production environment.

The Solution will be administered by a newly formed Policy Center lead by the Michigan State Police (MSP) and used by healthcare providers, law enforcement, and laboratories to whom kits are delivered for testing to track, among other things, the dates on which kits are: (1) collected by healthcare providers, (2) retrieved by law enforcement, (3) delivered by law enforcement to laboratories, and (4) tested by laboratories. Tribal jurisdictions and federal law enforcement are encouraged to use the system.

The Michigan Domestic and Sexual Violence Prevention and Treatment Board ("The Board") will be responsible to conduct an annual audit of the ongoing submission of kits and may, at its discretion, audit the functioning and use of the Track-Kit system as well. Healthcare providers, law enforcement, and laboratories will be included in the audit. Tribal jurisdictions and federal law enforcement are encouraged to participate.

Further, the Contractor will initially be expected to provide first line Online Chat and Phone Support; Option 4 - 24 hours a day, 365 days a year support to provide assistance and help to all users of the Solution as defined in Schedule B Service Level Agreement (SLA). See Implementation Section 4; 4.3.2 Support, for additional details.

This Solution will be implemented in three (3) Phases which is further defined in Section 4. Implementation:

1. Phase I – Discovery, Analysis and Design
2. Phase II – Pilot System
3. Phase III – Statewide Implementation and Roll-Out

2.2 Purpose

Michigan has passed legislation, Sexual Assault Evidence Kit Tracking and Reporting Act, MCL 752.962, that requires timely transfer of collected kits from the hospital to the law enforcement agency (LEA), from the LEA to the laboratory, and for turnaround from the laboratories. All entities covered by the Sexual Assault Kit Evidence Submission Act will be required to use the statewide electronic tracking system implemented by the state. Tribal jurisdictions and federal law enforcement are encouraged to participate.

This project will accomplish an entirely new business process and provide all stakeholders involved in the sexual assault kit processing workflow Statewide an efficient process to access information about kits electronically.

Several goals have been identified for this project and will be achieved by the Contractor's Solution: (1) a uniform statewide Solution to track the submission and status of sexual assault evidence kits (kits), with secure electronic access for victims, (2) auditing the ongoing submission of kits under the Sexual Assault Evidence Kit Submission Act, MCL 752.931-752.935.

3. SPECIFICATIONS

Known stakeholders involved Statewide using the Solution are:

1. Sexual assault victims

2. Kit manufacturer and/or distributor
3. Any accredited laboratory to whom the kits are sent for analysis
4. Law enforcement agencies
5. MSP including the Forensic Science Division (“MSP-FSD”)
6. Healthcare providers
7. Prosecuting attorneys for each Michigan County
8. The Board

3.1 Specification Overview

The following **Figure A** depicts the nine Track-Kit web portals which will be provided to the State out-of-the-box and configured, without additional cost, based on the technical and business specifications identified in this Contract with a high-level description of the feature set and functionality for each portal.

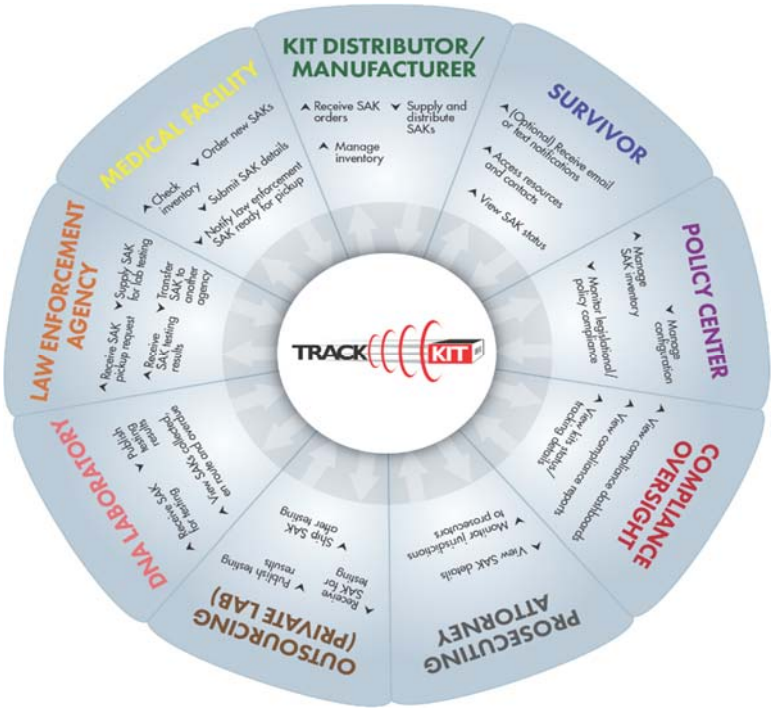

Figure A: Track-Kit Web Portals

The Track-Kit Portals
At a minimum, the users will be able to do the following via Track-Kit’s secure, password-protected web portal:

Survivor Portal

- Anonymously access the portal via mobile device or computer
- Opt-in to email or text message notifications
- View processing status
- Access survivor-based, location-specific resources such as websites, documents and contact information
- Access information in multiple languages (as supported)

Medical Facility Portal

- Capture collected kit information, including the bar code and by whom/where/when the kit was collected
- Specify if the survivor wishes to release the kit to law enforcement
- Notify law enforcement that the kit is ready for pickup
- Notify the lab that the kit has been collected
- Check inventory, order new kits, receive kits and destroy expired kits
- Generate kit collection reports

Law Enforcement Agency Portal

- Receive notifications that kits are ready for pick-up from a medical facility and/or DNA laboratory
- Record the date/time kits are picked up and delivered to/from the DNA laboratory
- Transfer kits to another agency
- Assign investigators and case numbers to kits
- Review lab conclusions and, at the State's discretion, release limited conclusion details to the survivor
- Generate reports related to kits that have been picked up
- Generate the manifest of kits sent to the private lab
- View the list of kits outsourced to a private lab, and their delivery, receipt and completion status
- Generate reports related to kits outsourced to private labs, their completion status and turnaround time

Prosecuting Attorney Portal

- Assign jurisdictions to prosecutors
- Review information on kits assigned to jurisdictions' agencies

DNA Laboratory Portal

- View the list of collected kits and those currently in route to the lab
- View the list of overdue kits and where they were collected
- Record the date/time kits are received from law enforcement agencies
- Document user-definable conclusions for each kit, such as (for example) profile obtained, CODIS hit, screening completed and case completed
- Receive notifications when a kit is nearing its processing deadline
- Generate notifications for kits ready to be picked up by an agency
- Generate reports on turnaround time and backlog
- View the list of kits outsourced to a private lab, and their delivery, receipt and completion status
- Generate reports related to kits outsourced to private labs, their completion status and turnaround time

Outsourcing (Private Lab) Portal

- View the list of kits in transit to the private lab
- View the list of kits received by the private lab
- View the list of kits completed by the private lab and not yet received by an agency
- Generate reports on the kits received, completed and turnaround time

Kit Distributor Portal

- Receive kits from the manufacturer
- Manage inventory
- Receive orders and ship kits to medical facilities and agencies
- Generate order reports
- Generate barcodes

Compliance Oversight

- Generate dashboards and reports aimed at evaluating compliance of stakeholders (where applicable) to state legislation.
- View detailed local and statewide kits status and tracking details

Policy Center Portal—used to set the rules, configuration, roles and permissions for the system

- Set thresholds for notification
- Define portal roles and manage security, access rights and user accounts
- Manage kit analysis conclusions that can be made available to survivors
- Provide survivors access to resources based on their location and in their language
- Define performance metrics displayed in each portal-specific dashboard
- Post and manage bulletin board entries for each portal
- Manage kit inventory—reconcile kit orders, inventory, distribution, submission, receipt and destruction
- Generate reports on user activity, auditing records and jurisdiction-wide kit inventory

- Generate Management/Admin Reports

Figure B provides a high-level architecture of Track-Kit and illustrates the interaction of technologies and the relationship between the various components of the Solution.

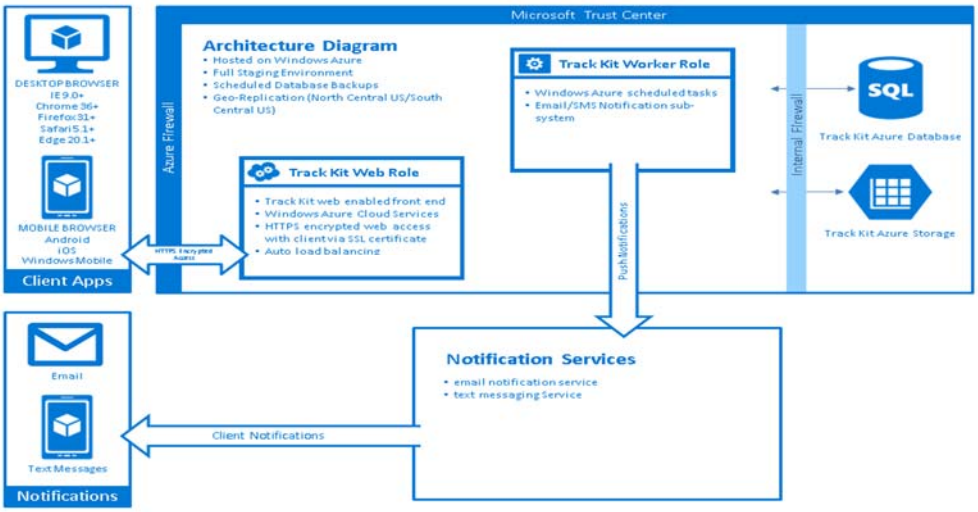

Figure B: Track-Kit System Components and Technologies

3.2 Business Specifications

See Schedule A - Table 1 Business Specifications for specified business requirements.

3.2.1 User Type

The proposed access types, which will be finalized with the Contractor during Phase I, are defined below:

a. Read Only – Logs into the Solution and views the status and location of their SAEK; exclusively held by survivors.

b. User Read Only – Logs into the Solution with secured login using UserID and Password to view the status and location of kits in the Solution by manually entering the SAEK barcode number; the primary users will be prosecutors.

c. Write Access with Scanner – Logs into the Solution with secured login to update the location or status of a SAEK via data entry and / or barcode scanner.

d. Write Access without Scanner – Logs into the Solution with secured login to update the location or status of a SAEK via data entry. The primary users will be detectives and some MSP Crime Lab personnel.

e. Solution Administrator – Logs into the Solution with secured login to track all SAEKs in the local jurisdiction, run reports, reset user access, and add / remove Solution users.

f. Super User – Logs into the Solution with full ability to administer the Solution including making configuration changes, running reports, resetting user access, adding / removing Solution users, overseeing general Solution performance.

Table A identifies several attributes of the Solution usage. For each entity / agency that will have access to the Solution, Table A identifies the users of the Solution, whether barcode scanning is needed, access type, actions performed by each group, and estimations of number of users:

TABLE A

Entities / Agency	Users	Barcode Scanner Needed?	Access Type	Actions Performed	Approximate # of Users
N/A	Survivors	No	Read Only	Track SAEK location / status	Unknown
Medical Facilities	SANEs	Optional	Write Access with Scanner	Initial data entry of SAEK	~150-250
LEAs	Detectives / Officers / Deputies	Optional	Write Access without Scanner	Update SAEK location / status	~100-200
LEA Property / Evidence Management	Officers / Deputies / Sergeants	Optional	Write Access with Scanner	Update SAEK location / status	~600
MSP Crime Lab Property and Evidence	Assigned lab evidence control staff	Optional	Write Access with Scanner	Update SAEK location / status	~20-25
MSP Crime Lab	Additional MSP personnel who process RFLEs	No	Write Access without Scanner	Update SAEK location / status	~10
Prosecutors	Deputy Prosecutors / Paralegals	No	User Read Only	Track SAEK location / status	~200
Solution Administrators	Assigned personnel in medical facilities, LEAs, and MSP	No	Solution Administrator	Manage users in District / local jurisdiction	~100-125
MSP Super Users	Assigned personnel	No	Super User	Manage all Solution administration	~5-10

Note: The Contractor will not be responsible for installing the barcode scanners, which are optional to use by the specified users above.

3.3 Technical Specifications

3.3.1 Specific Standards and/or Certifications

3.3.1.1 Enterprise IT Policies, Standards and Procedures

All services and products provided by the Contractor must comply with all applicable State IT policies and standards listed at:
Enterprise IT Policies, Standards and Procedures: http://michigan.gov/dtmb/0,4568,7-150-56355_56579_56755---,00.html

3.3.1.2 Look and Feel Standard

All software items provided by the Contractor must adhere to the Look and Feel Standards: www.michigan.gov/somlookandfeelstandards.

3.3.1.3 Federation/Single Sign-on (SSO)

Solution must be capable of supporting the State standard federated single sign on with multi-factor authentication using SAML or comparable mechanisms during Phase I Discovery, Analysis and Design.

3.3.2 End-User Operating Environment

Below is the initial end user operating environment that must be supported by the Contractor. Contractor is expected to keep pace with changes in standard operating environments (e.g. operating system upgrades, web browser upgrades, mobile OS upgrades).

The Solution must not use any specialized or proprietary hardware, devices and/or computers.

The Solution will not use any plugins and will not require Java, Flash, or Silverlight.

3.3.2.1 Web Browsers

Solution must run under commonly used web browsers. At a minimum, the software must support Internet Explorer v9+, Chrome v36+, Firefox v31+, Safari v5.1+, and Edge 20.1+ under the Windows and iOS operating Solutions.

3.3.2.2 Mobile

The Solution must utilize responsive design practices to ensure the application is accessible via a mobile device. Solution must support iOS, Android and Windows Mobile platforms for mobile devices (e.g. cellular phones and tablets). All features and functions of the Track-Kit must be able to perform via mobile devices.

3.3.3 Security

Contractor agrees and must comply with the Data Security requirements set forth in Schedule F – Data Security Terms and Schedule E – Disaster Recovery Plan.

Due to the Solution storing sensitive data, the Contractor and its Solution must comply with the following:

a. Solution must be hosted in an Azure Government Cloud located in the continental U.S. which is a FedRAMP certified facility. The Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are 2 hours.

b. Remain compliant with the NIST Special Publication 800.53 (most recent version) MOD controls. On a quarterly basis, the Contractor will review the NIST Special Publication 800.53 (most recent version) MOD for any updates or changes and implement those that apply to the Solution.

c. Be encrypted at rest and in flight using AES 256 bit or higher encryption, including database backups. The transport layer between the client's web browser and the web server must be encrypted using TLS 1.2 connection with AES 256-bit certificate. The application model view control architecture must protect against SQL injection attacks and has internal firewall to validate database connections from the web server to the database. The Solution must also have additional built-in security to validate that a jurisdiction only has access to that jurisdictions' data.

d. Provide multi-factor authentication. This level; however, does not require a hard token at contract execution. Some other method such as SMMS text with passcode, phone call with temporary passcode or other approved multi-factor authentication method must be used. The Solution as of October 2017 is architected to support multi-factor authentication; however, it has not been implemented due the vast range of users including survivors. Multi-factor authentication functionality for actual user types will be provided as the State requires during Phase I of the project.

e. Remain compliant with the Health Insurance Portability and Accountability Act (HIPAA) Policies. On a quarterly basis, the Contractor will review the HIPAA policies for any updates or changes and implement those that apply.

3.3.4 Capacity

The Solution must automatically provide, at no additional cost, additional resources as the level of concurrent users increases without affecting performance as defined in Schedule B – SLA, Section 4.4. Software Response Time.

3.3.5 Access Control and Audit

a. All user activities must be tracked within the Solution and accessible to administrative users via reports except that victims accessing the system will not be tracked by user identity.

b. The Solution must contain full web-based user and data management capabilities for local site administration as well as remote site administration through the Policy Center.

3.3.6 Data Migration

There are no migration services known at contract execution, however the State may need migration services in the future.

3.3.7 Data Retention

Since the Solution will be deployed in the Contractor's Azure Government cloud it will have no database storage limitations, duration or maximum retention period. All Solution data will be readily available for reporting and auditing purposes with no impact on pricing.

3.3.8 System Integration

The Solution must publish APIs though a Contractor web service to allow communication between the Solution and any current or future third-party applications that may need to share data.

For Phase I and II, the Solution must integrate with the MSP-FSD Laboratory Case Management System (LCMS), an existing database-driven application currently in use. The LCMS will push SAEK data to the Contractor's web service when the LCMS receives kits into the laboratory and returns kits from the laboratory.

Since this approach has the LCMS pushing data to the Solution in real time as updates happen in the Solution, it guarantees that the information relayed by the Solution will be up to date with what the LCMS has in its records.

4. IMPLEMENTATION

The following describes the high-level approach and methodology the Contractor will employ to meet the business and technical specifications.

As stated earlier, this project will be broken into three main phases and aligns with the Preliminary Project Schedule found as Exhibit A.

- Phase I – Discovery, Analysis and Design
- Phase II – Pilot Solution
- Phase III – Statewide Implementation and Roll-Out

The Solution must be tested and ready for Acceptance for use Statewide within 120 days following contract execution.

4.1 Phase I - Discovery, Analysis and Design

The Discovery, Analysis and Design phase will focus on knowledge transfer between the State and Contractor. The Discovery, Analysis and Design phase will focus on the outcome of the gap analysis, thus identifying incremental Track-Kit enhancements required to fully meet the business and technical requirements herein. This becomes the new requirements baseline, or end product.

4.1.1 Implementation Plan

The Final Implementation Plan will be delivered within (30) days following Contract Execution. See Project Management Approach in Section 5. Milestones and Deliverables for further details.

4.1.2 Gap Analysis

A detailed analysis of the State's requirements will be conducted to determine the optimal configuration and customizations of the Solution.

Track-Kit is highly configurable by design. This key characteristic allows jurisdictions to control the behavior of the software to meet the business and technical requirements.

Contractor will be responsible for performing the configuration of the Solution for implementation. This task will be broken into two components: Configuration Settings and Seed Data. The State must be trained and able to maintain and manage all Configuration Settings and Seed Data without any assistance from the Contractor after implementation. This also includes, but not limited to dashboards and reports. In the case the State requires assistance in maintaining and managing the Solution the Contractor will provide assistance at no additional cost.

Configuration Settings:

Contractor will configure the following:

1. Notification Types
2. Spanish Translations for the Survivor portal
3. "Help" indicators descriptions
4. Roles and Access Rights for each portal
5. Policy Center user accounts
6. SAEK conclusions
7. User Defined Fields (UDFs)
8. Solution Settings

Seed Data:

Using MS-Excel templates for bulk data load, Contractor will populate the following data:

1. Code tables:
    a. State
    b. County
    c. City
2. All portal sites
3. For each portal site:
    a. Primary contact information
    b. All portal user accounts (excluding the Policy Center portal)
    c. Notification recipient email addresses
    d. Survivor resources
    e. Bulletin board messages

The first step will be to assess and document the gaps between the stated requirements and the features and functionality currently available in Track-Kit out-of-the-box – the initial baseline. Using Track-Kit and the State's requirement as the frame of reference, the project team will document the delta (the gap) between both components.

The Business Analyst Lead will perform a Gap Analysis by facilitating Joint Application Design (JAD) sessions that will identify any incomplete, ambiguous or conflicting requirements. This analysis will ensure

that specific project requirements and deliverables, defined by the Contract, are included in the project design specifications.

The outcome (Gap Analysis Report) will constitute the basis for driving the Track-Kit software customization requirements. Contractor will then define the customization Solution requirements and using an Agile Framework Contractor will follow through with the actual software customization work combined with unit and integration testing of the resulting Solution.

At the completion of the Gap Analysis, the Business Analyst Lead will issue a Final Scope and Assessment Report to the State.

This process will be done by the Contractor Business Analyst Lead facilitating JAD sessions held with the State at the State's location to discuss any incomplete, ambiguous or conflicting requirements. During consultations with the State, Contractor will identify and recommend alternatives for addressing the identified gaps and implement changes accordingly, taking into consideration schedule and budget constraints.

Based on the outcome of the findings and consultations, the Business Analyst Lead will issue a Final Scope and Assessment Report to the State.

Once the Scope and Assessment Report is agreed between both Parties, the Contractor' Business Analyst Lead and the Contractor's Project Manager will provide and obtain State approval for the Final Project Schedule and confirmed budget.

4.1.3 Customization and Testing

The Customization and Testing stage will be executed using an Agile framework to produce rapid incremental milestones.

The Preliminary Project Schedule as Exhibit A has provisions for two (2) Sprints but may need to be adjusted depending on the findings from the Gap Analysis stage at no additional cost.

Using Scrum methodology, the Contractor will break down the software customization effort into two to three-week duration sprints depending on the nature of the customizations to be developed.

At a high-level, each sprint will be made up of four main streams:

- Solution Requirements Definition;
- Software Customization;
- Quality Assurance (QA)/ Testing; and
- User Documentation.

4.1.3.1 Solution Requirements Definition

The Solution Requirements Definition stream will be spearheaded by the Contractor's Business Analyst and the Contractor's Development Lead will participate to assess and report any technical impact. This stream will require direct interaction with subject matter experts from the State to communicate the detailed requirements to the Contractor. The Deliverables from this stream will be the baseline Solution requirements which constitute the formal input to the Software Customization stream.

4.1.3.2 Software Customization

The Software Customization Stream will encompass all the activities related to the actual customization of Track-Kit. As the Contractor performs those activities, "review points" will be established to demonstrate to the State the customization work accomplished to date. The "review points", will be scheduled by the State and Contractor Project Managers. The Subject Matter Experts of the State will participate in the review point sessions as required.

The high-level work effort of the Contractor's resources during this stream is:

- Business Analyst Lead: schedules reviews with the software development team to ensure compliance with the baseline Solution requirements.

- Software Development Lead: directs and manages the daily software engineering activities
- Software Developers: perform the actual software engineering work in accordance with the baseline Solution requirements.
- QA Analyst: generates all test cases based on the baseline Solution requirements and performs all Solution tests.

4.1.3.3 Quality Assurance (QA) / Testing

Contractor agrees with Acceptance Testing; Acceptance requirements set forth in the Contract Terms Section 13.

Unit, functional, regression and performance testing of the entire Solution will be performed by the Contractor.

Contractor will use its Axosoft management platform to document all the activities pertaining to unit, functional, regression and performance testing of the entire Solution. Contractor QA team will use the requirements baselines as the frame of reference for devising Test Plans and detailed Test Cases as part of the Implementation Plan to confirm that all developed Solution features and functionality meet the Acceptance criteria.

If the development does not fully meet the expected results, then an Incident (aka Ticket) will be generated in Axosoft's management platform. Incidents are qualified either as a "Defect", "Change Request" or "Support" and can be in any of the following states (workflow step):

- Incident reported (default workflow step of a newly created Incident)
- Incident being fixed (the assigned developer is currently working on the identified issue)
- Incident – duplicate (no action required – this Incident has already been reported)
- Incident – not an issue (does not require any further action)
- Incident released to QA (the assigned developer fixed the defect and released the Incident to the QA team for final testing)
- Incident verified (indicates that the development successfully met the conditions as specified in the test case(s))

For each Incident reported ("Defect"), the assigned Contractor QA analyst provides detailed diagnostic information as a way to fully document the findings and inform the assigned Contractor developer. The diagnostic information will contain:

- The area of the software where the defect was encountered (e.g. Module "A", Data entry form "B")
- Detailed description of defect
- Detailed steps to reproduce the defect

Axosoft's management platform will ensure that up-to-date information is maintained throughout the iterative Solution development and testing cycles.

After all test cases are successfully executed, the final build is released to the State for user acceptance testing (UAT). Contractor will work with the State to perform all UAT testing activities. Should issues be encountered during UAT then the State (with the support of Contractor as required) will use Axosoft's management platform to submit Incidents. Those Incidents will be managed as per the process described above and successfully corrected by the Contractor before Phase II can commence and at no additional cost to the State.

4.1.3.4 User Documentation

The Contractor's user documentation must provide detailed information about all software features and functionality, enabling the State to resolve common questions and issues prior to initiating formal support requests to the Contractor.
The Contractor must develop and submit for State approval complete, accurate, and timely solution documentation to support all users, and will update any discrepancies, or errors through the life of the contract. Contractor will also update any areas of the documentation impacted when new releases of the Solution are made available to the user community throughout the life of the contract.

4.1.4 Train-the-Trainer Training

Contractor will provide the State with on-site Train-the-Trainer in one session (up to 4 days onsite) for 8 to 10 users/trainers and with initial end-user training as set out in this section. The State is responsible for continuing delivery of training to end-users during and after Phase III. Contractor must provide training material to the State for delivering user training across all Solution User Groups as listed below and as described in Section 4.3.1. All Policy Center and Compliance Oversight users (who will be referred to as "Super Users" throughout this section) will develop a complete understanding of each portal type and the overall Solution workflow. The Contractor will provide the State a Final Training Plan including the training curriculum for acceptance before training commences.

Training Curriculum

Track-Kit training courses described below is an overview for each Solution User Groups and for each type of users. The training curriculum may be tailored in the Final Training Plan accepted by the State.

Training Course #1: Track-Kit Overview

Audience: Super Users, Solution Administrators and End-Users from Medical Facilities, Law Enforcement Agencies, Crime Labs, and Prosecutors

Course Title	Course Abstract
Introduction to Track-Kit	This introduction will help users understand the purpose of Track-Kit in their place of work, both as a whole and in their regular day-to-day tasks. Users will get an overview of the Track-Kit workflow, and learn how to navigate through the software and how to enter or edit data. Users will also learn about Track-Kit's common elements such as: • Worklists (grids) and how they can easily be filtered or exported in a variety of formats (Print, PDF, CSV and XLS) • "Contact Us" form for user inquiries • Search for help using the FAQs (Frequently Asked Questions) and Online Help • Increase/Decrease font sizes • User profile and account settings • Configuring and Generating Reports (Super Users and Solution Administrators only)

Training Course #2: Using the Policy Center and Compliance Oversight Portals

Audience: Super Users

Course Title	Course Abstract

Managing Bulletin Board Messages	Users will learn how to manage bulletin board messages, which are displayed at the top of each portal's home page. Users will also learn how to customize each message by specifying its portal type, portal site, activation date and (optionally) a deactivation date.
Managing Conclusions (Processing Details and Results)	Users will learn how to manage conclusions, which are used by laboratory technicians to indicate whether DNA results are positive or negative. Users will also learn how to specify each conclusion's display order and how to deactivate conclusions that are no longer required.
Managing FAQs	Users will learn how to manage frequently asked questions, which can be set to be displayed to one or more specific portal types. For each entry, users will learn how to specify a question, an answer and their display order.
Managing User Inquiries	Users will learn how to view and deactivate user inquiries, which are listed on the "User Support" page and organized in chronological order.
Managing Notification Recipients	Users will learn how to manage notification recipients and their subscriptions to Solution notifications.
Managing Resource Groups	Users will learn how to manage resource groups, including each group's individual resources. Users will also learn how to specify a resource group's display order and its relevant states, counties or cities.
Managing Portals	Users will learn how to view, filter and search through all kits in Track-Kit. Users will learn how to view, filter and search through all orders in Track-Kit. Users will learn how to manage portal roles by assigning/unassigning the ability to perform general and administrative activities. Users will learn how to manage portal sites and their primary contacts, including how to update and re-configure site-specific settings. Users will learn how to manage any of Track-Kit's users, including the ability to update passwords and assign/unassign pre-defined roles.
Generating Reports	Users will learn how to configure and generate reports. Users will also learn how to customize reports by applying report-specific filters (such as Locations, Users, Date Ranges, etc.)
Managing Code Tables and Solution Settings	Users will learn how to manage code tables, which are lists of closely related items used throughout the Track-Kit software (e.g. Cities, Counties, Problem Kit Reasons, etc.). Users will also learn how to manage Solution settings, which are absolutely essential to the software's performance.
Managing Terminologies	Users will learn how to manage and customize terminologies that are used throughout the software, including the wording for: • Activity Types • Code Tables • Conclusions (Processing Results) • Dashboards (Charts and Graphics) • Discard Reasons • Help Bubbles (Tool Tips) • Kit Statuses • Notifications

	• Reports

Training Course #3: Using the Medical Facility Portal

Audience: Super Users, Solution Administrators and Medical Facility Portal End-Users

Course Title	Course Abstract
Viewing Orders and Receiving Shipments from Distributors	Users will learn how to view outstanding distributor orders and how to receive each order's incoming shipments.
Receiving Unexpected Kits	Users will learn how to receive kits into their inventory using the "Kit Receipt Wizard", which allows them to enter or scan individual barcodes. Users will also learn how to set the kits' "Expiration Date".
Collecting Kits	Users will learn how to collect kits from their uncollected inventory. This is done by selecting an uncollected kit and filling out its "Kit Details" page, which allows them to release the kit and assign it to a law enforcement agency. Users will also learn how to complete additional fields, such as the "Collector" and "Collection Date" fields.
Discarding Kits	Users will learn how to discard kits from their inventory.
Generating Reports	Users will learn how to configure and generate reports. Users will also learn how to customize reports by applying report-specific filters (such as Locations, Users, Date Ranges, etc.).
Missing Information Kits	Users will learn how to manage and update kits with missing information.
Solution Administrator Tasks	The Solution Administrator(s) of the Medical Facility will learn how to update or re-configure the following for their site: • Contact Information • Associated Agencies • Users • Notifications and Notification Recipients • Bulletin Board Messages • Portal Site Settings

Training Course #4: Using the Law Enforcement Agency Portal

Audience: Super Users, Solution Administrators and Law Enforcement Agency Portal End-Users

Course Title	Course Abstract
Picking Up Kits from Medical Facilities	Users will learn how to pick up kits from medical facilities using the "Kit Pickup Wizard", which allows them to view a kit's details before proceeding. Users will also learn how to complete additional fields, such as the "Pickup Date", "Pickup Officer", "Assigned Officer" and "Case Number" fields.
Picking Up Kits from Laboratories	Users will learn how to pick up kits from laboratories using the "Kit Pickup Wizard", which allows them to view a kit's details before proceeding. Users will also learn how to complete additional fields, such as the "Pickup Date", "Pickup Officer", "Assigned Officer" and "Case Number" fields.
Managing Kit Transfers and Outsourcing to Private Labs	Users will learn how to transfer kits from one law enforcement agency to another, how to accept incoming kit transfers and how to outsource kits to private labs.

Managing Survivor Access to Kit Location	Users will learn how to manage survivor access to the status and location of the kits , which can be found on the “Action Required” worklist or from a kit’s details page.
Generating Reports	Users will learn how to configure and generate reports. Users will also learn how to customize reports by applying report-specific filters (such as Locations, Users, Date Ranges, etc.).
Solution Administrator Tasks	The Solution Administrator(s) of the Law Enforcement Agency will learn how to update or re-configure the following for their site: • Contact Information • Associated Agencies • Users • Notifications and Notification Recipients • Bulletin Board Messages • Portal Site Settings

Training Course #5: Using the Laboratory Portal

Audience: Super Users, Solution Administrators and Laboratory Portal End-Users

Course Title	Course Abstract
Receiving Kits from Law Enforcement	Users will learn how to receive kits from law enforcement agencies using the “Kit Receipt Wizard”, which allows them to view a kit’s details before proceeding. Users will also learn how to complete additional fields, such as the “Lab Case Number” and the “Submission Date” fields.
Managing Processing Details	Users will learn how to manage a kit’s processing details using the “Processing Details Wizard”, which allows them to view a kit’s details before proceeding. Users will also learn how to complete additional fields, such as indicating test results, processing dates and notifying law enforcement agencies once a kit is ready for pickup.
Outsourcing to Private Labs	Users will learn how to outsource kits to private labs.
Generating Reports	Users will learn how to configure and generate reports. Users will also learn how to customize reports by applying report-specific filters (such as Locations, Users, Date Ranges, etc.).
Solution Administrator Tasks	The Solution Administrator(s) of the Laboratory will learn how to update or re-configure the following for their site: • Contact Information • Users • Bulletin Board Messages

Training Course #6: Using the Prosecutor Portal

Audience: Super Users, Solution Administrators and Prosecutor Portal End-Users

Course Title	Course Abstract
Finding Kits	Users will learn how to view, filter and search through all kits specific to their assigned county.

Generating Reports	Users will learn how to configure and generate reports. Users will also learn how to customize reports by applying report-specific filters (such as Locations, Users, Date Ranges, etc.).

Training Course #7: Using the Private Lab Portal

Audience: Super Users, Solution Administrators and Private Lab Portal End-Users

Course Title	Course Abstract
Receiving Kits from Law Enforcement or Laboratories	Users will learn how to receive kits from law enforcement agencies or laboratories using the "Kit Receipt Wizard", which allows them to view a kit's details before proceeding.
Completing Kits	Users will learn how to complete a kit's processing using the "Kit Processing Completion Wizard", which allows them to view a kit's details before proceeding.
Shipping Kits	Users will learn how to ship kits to a law enforcement agency or to a laboratory using the "Kit Shipment Wizard", which allows them to view a kit's details before proceeding.
Generating Reports	Users will learn how to configure and generate reports. Users will also learn how to customize reports by applying report-specific filters (such as Locations, Users, Date Ranges, etc.).
Solution Administrator Tasks	The Solution Administrator(s) of the Private Laboratory will learn how to update or re-configure the following for their site: • Contact Information • Users • Bulletin Board Messages

Training Course #8: Using the Kit Distributor Portal

Audience: Super Users, Solution Administrators and Prosecutor Portal End-Users

Course Title	Course Abstract
Receiving Inventory from Manufacturers	Users will learn how to receive kits from manufacturers using the "Lot Receipt Wizard", which allows them to enter/scan case barcodes or to enter barcode ranges. Users will also learn how to complete additional fields, such as the "Lot Number", "Expiration Date" and "Lot Receipt Date" fields.
Filling Order Requests	Users will learn how to fill order requests for medical facilities using the "Fill Order Wizard", which allows them to enter/scan case barcodes or to enter barcode ranges. Users will also learn how to complete additional fields, such as the "Courier" and "Tracking Number".
Rejecting Kits	Users will learn how to reject kits from their inventory using the "Kit Rejection Wizard", which allows them to enter/scan barcode ranges or to enter/scan individual barcodes. Users will also learn how to complete additional fields, such as the "Reject Reason" and "Reject Comments" fields.
Generating Reports	Users will learn how to configure and generate reports. Users will also learn how to customize reports by applying report-specific filters (such as Locations, Users, Date Ranges, etc.).
Solution Administrator Tasks	The Solution Administrator(s) of the Kit Distributor will learn how to update or re-configure the following for their site:

	• Contact Information • Users • Notifications and Notifications Recipients • Bulletin Board Messages • Portal Site Settings

4.2 Phase II – Pilot Solution

The proposed pilot Solution phase will allow for managing risk, validate (revalidate) the features and functionality provided by the pilot Solution and address change to be delivered prior to Phase III.

One jurisdiction as identified by the State will be utilized for Phase II.

The Contractor will work with and support the State in the development of the pilot approach, planning and provisioning of the pilot environment, ongoing monitoring of the pilot Solution and finally assessing its success prior to implementing Phase III, a Final Pilot Approach Plan.

Contractor and State work together to:

- Determine the goals and expectations of the pilot project
- Provide pilot user training
- Develop the approach for monitoring ongoing operation of the pilot Solution from a user perspective by:
    - Gathering user feedback
    - Maintaining momentum
- Evaluate the pilot project
    - Define the success factors
    - Identify the variables to be measured
    - Debrief at the end of the pilot (collect feedback and lessons learned)

Further the Contractor will be responsible for providing Support to all pilot users of the Solution as defined below in Section 4.3.2 Support.

4.3 Phase III – Statewide Implementation Rollout

The Solution will ultimately be deployed to and will impact hundreds of State organizations and thousands of State users. Accordingly, the Contractor will work with and support the State in the development of a Roll-out Plan. The parties will create a joint a Roll-out Plan to communicate the strategic deployment of Phase III. This Roll-out Plan must be finalized, prior to implementing Phase III.

While the State will be responsible for the delivery of training to end-users (except for victims), the Contractor will provide assistance as defined in Section 4.3.1 Webinar-based Training and the necessary training materials to allow for all types of users to teach themselves independently without any additional support.

The Contractor will provide a 90-day warranty period once the Solution is implemented Statewide and will be responsible for providing Support as defined in Section 4.3.2 Support to all users of the Solution during this time and ongoing after Final Acceptance.

4.3.1 Webinar-based Training

At no additional cost to the State, the Contractor will assist the State in providing regular webinar-based end-user training for six months starting on day 1 of the statewide implementation of the Solution.

Contractor will assist the State in delivering scheduled/rotational training webinars to SAEK Distributor, Medical Facility, Law Enforcement Agency, Prosecuting Attorney, Laboratory and Outsourcing (Private Lab) portal end-users. Contractor will record training sessions in the initial stages of training delivery for reuse (as training videos accessible online through the Solution) by the Solution user community on an as-needed basis. This training must continue to be made available online throughout the life of the contract, and the

Contractor will revise or update these webinars at the time the Contractor makes revisions or updates to the Solution to ensure the recorded training is current.

The frequency/schedule of the training webinars will take into account the overall number of end-users per stakeholder group and the actual Roll-out Plan of the Solution jurisdiction-wide.

The State will facilitate the training webinars using the Contractor provided training material for delivering user training across all Solution User Groups and should include a formal presentation covering all aspects of the Solution based on the audience (Regular users and Admin users) followed by a Q&A session.

If development and delivery of additional ongoing training beyond the initial implementation of phase III is to be delivered by the Contractor, fixed-price fees will apply per Schedule D – Pricing.

4.3.2 Support

Contractor must comply with Schedule B - Service Level Agreement during Phase II and Phase III, and:

a. The Contractor provides multiple end-user support tiers as defined below. The State will initially require Online Chat and Phone Support; Option 4 - 24 hours a day, 365 days a year as it's selected end-user support option. The Contractor will accommodate the State if the State elects a different support tier within 90 days of written notice from the State Contract Administrator via executed contract change notice. Costs will be adjusted according to Schedule D – Pricing.

    i. Online Chat Only

        1. Option 1 - 8 a.m. – 5 p.m. Monday through Friday
        2. Option 2 - Extended business hours Monday through Friday (6h00-21h00)
        3. Option 3 - Extended business hours - 365 days a year (6h00-21h00)
        4. Option 4 - 24 hours a day, 365 days a year

    ii. Online Chat and Phone Support

        1. Option 1 - 8 a.m. – 5 p.m. Monday through Friday
        2. Option 2 - Extended business hours Monday through Friday (6h00-21h00)
        3. Option 3 - Extended business hours - 365 days a year (6h00-21h00)
        4. Option 4 - 24 hours a day, 365 days a year

b. The Solution will actively monitor and record the following performance metrics; CPU Percentage, Disk Read/Writes, and Network In/Out activity. The Solution will actively monitor and record response time for all resource requests on the server, actively monitors and records Solution and resource failures.

c. Solution availability will be monitored every 5 minutes from 5 different locations spread around the continental United States. An alert notification will be sent to the Contractor support team in the event of a failure at any 3 locations within the 5 minute timeframe.

d. Each maintenance release and/or hot fix of the Solution must be planned, documented in the Solutions requirements document(s), and have been validated by the Contractor QA team to ensure compliance with the baseline requirements. Contractor will notify the State a minimum of 14 days in advance of a scheduled maintenance release and/or hot fix.

    Once the release has passed validation it is ready to be rolled out to the State's test environment. The State will then have the opportunity to review the changes and if Solution works accordingly it will be rolled into production at an agreed time. Release notes detailing the changes/upgrades that are included in the software release will be provided by the Contractor. The Release notes will identify reported bug fixes and new features and functionality as part of the new release.

e. Contractor will update all user documentation that requires updating with each new release of the Solution.

5. MILESTONES AND DELIVERABLES

This project will be broken into three main phases and the Milestones and Deliverables aligns with the Preliminary Project Schedule found as Exhibit A and the Pricing in Schedule D. The Solution must be implemented Statewide within 120 days following contract execution.

5.1 Project Management Approach

In managing its obligation to meet the milestones and deliverables in the Final Implementation Plan, the Contractor will assist the State in completing any State Unified Information Technology Environment (SUITE) documentation requested by the State. The State reserves the right to give final approval of any substituted documents the Contractor may propose in its place.

The Contractor will use a Company Standard Procedure for Project Management (CSP-PM). The CSP-PM combines Agile software development methodologies with guidance from the PMBOK and is tailored to the Contractor products and services. Contractor methodology primary goal (like the SUITE methodology) is to deliver projects and products on time, on budget and most importantly with a level of quality that meet the Customer's satisfaction.

The Final Implementation Plan will define all aspects of the management process including:

A. Management Team Roles and Responsibilities
B. Scope Definition and Control
C. Planning and Scheduling
D. Project Meetings
E. Cost Control
F. Quality and Validation
G. Communications
H. Risk Management
I. Issues Management
J. Project Closeout

All documentation related to the Project will be maintained using Contractor's Axosoft management platform and its corresponding Customer Portal that will be accessible to the State users decided by the State.

Below is a high-level description of each aspect expectation of the management process to support this project.

5.1.1 A - Management Team Roles and Responsibilities

The management team will be comprised of the Contractor Key Personnel listed in Section 8. Contractor Key Personnel. Contractor responsibilities are listed within the SOW and will be specifically detailed for every Phase of this project in the Final Implementation Plan.

5.1.2 B - Scope Definition and Control

5.1.2.1 Project Scope

Within (5) days, after contract award, the Contractor Project Manager will work with the designated State Project Manager to schedule a kick-off meeting at a State site location to reconfirm the Solution scope as defined in this Contract.

The Contractor's Customer Portal (a component of the Contractor's Axosoft management platform) will allow the State to monitor the project status and progress. The State will be able to view real time project progress, feature and functionality development, test results and incident rectification.

5.1.2.2 Change Management

Changes to scope, schedule, or cost must be addressed through a formal change request process with the State and the Contractor to ensure understanding, agreement and approval of authorized party(s) to the change and clearly identify the impact to the overall project.

Contractor will use its Axosoft management platform and its corresponding Customer Portal to communicate, assess, monitor, and control all changes to the project.

Contractor's Project Manager will be responsible and accountable for the management of the project scope (creep or reduction). Change requests, which change the requirements of the Solution initially measured against the final set of baseline Solution requirements, will be formally documented. The revised Solution requirements will form the foundation for the remainder of the project and any further change requests.

5.1.2.3 Change management Log

This change management log will be continually updated throughout the project and the Contractor Project Manager will be accountable for ensuring that only approved changes to this base are incorporated into the Solution.

The processes for managing change is as follows:

- Change Requests (CRs) submitted via the Customer Portal is the vehicle for communicating changes. Each CR must describe the nature of the change, the rationale for the change, and finally the impact that the requested change will have on the project
- Once submitted, the CR will be reviewed by the Project Managers from both parties in order to either reject the change or approve it for further investigation
    - If approved for further investigation Contractor's Project Manager will inform the client of the charges for conducting the investigation (see Schedule D - Pricing), if applicable.
    - Once completed the investigation will determine the impact of implementing the requested change; i.e. the impact it will have on price and project schedule.
    - A written and signed contract change notice with both parties is required by both parties before any work in relation to the CR is initiated, if cost is impacted.

5.1.3 C - Planning and Scheduling

The Contractor Project Manager will assign all the appropriate resources to the project and will monitor schedule performance on a continuous basis. Achievement dates will be tracked to determine the impact on schedule milestones.

The Contractor Project Manager will identify and track the schedule's critical path, develop mitigation plans to address the critical path and issue weekly project schedule updates to the Project Team.

The Contractor Software Development Lead is responsible for monitoring the design activity, verifying compliance with the schedule and determining acceptable solutions to any potential schedule risk. This resource will also ensure that State's technical project requirements are fully addressed and incorporated into the software development. Further, this resource will advise the Contract Project Manager of any design activity schedule risks.

5.1.4 D - Project Meetings

5.1.4.1 Weekly Status Meetings

The Contractor Project Manager and other appropriate Key Personnel will attend weekly status meetings with the State Project Manager and other members of the State during the Project at a date and time mutually agreed upon in the Implementation Plan. These meetings will follow a pre-set agenda jointly prepared by the Contractor Project Manager and State Project Manager, but will also allow both Contractor and State to discuss other issues that may concern either party.

Contractor will provide brief written status reports at least 24 hours prior to the weekly status meetings. Status reports will describe the previous week's activities, including Deficiencies encountered and their disposition, results of tests, whether or not deadlines were met, and any Deficiencies that may have arisen that need to be addressed before proceeding to the next activities. The report will also describe the anticipated activities for the current week and any changes to project risks and risk mitigations. All Reports will be produced in formats and with the level of detail approved by the State and delivered in accordance with the terms of this Contract.

It is anticipated that most of the Weekly Status Meetings can be held via conference call, but Contractor will be onsite if required.

5.1.4.2 Project Team Meetings

The Contractor Project Manager will organize and chair monthly meetings with the State to discuss project tasks, schedules, progress and issues. The meetings also allow the project team to identify and resolve issues and potential conflicts. Action plans will be created and solutions monitored by the Contractor.

Contractor will produce a monthly report summary that compares actual performance of the Services (including but not limited to activities related to Deliverables) to budgeted charges and dates in the Final Project Schedule. The report will be submitted by Contractor's Project Manager to the State's Project Manager no later than the last work day of each month. The monthly report will address at minimum:

1. Summary of activity during the report period
2. Accomplishments during the report period
3. Deliverable status
4. Schedule status
5. Action Item status
6. Repair status
7. Maintenance activities

5.1.4.3 Quarterly Review Meetings

The Contractor senior management along with the Contractor's Project Manager shall facilitate, at a minimum, quarterly review meeting with State Stakeholders and additional meetings at other times as agreed upon by the parties. The Contractor will report on the status of the Project, progress in completing the Implementation Plan, issues and risks on the Project, and plans to resolve outstanding issues, if any.

5.1.5 E - Cost Control

See Section 10. Pricing for cost and credit details.

The implementation of the Solution, Phase I – III, will be on a fixed-price basis as defined in Schedule D - Pricing.

For new development after Phase III, the State will be enrolled into the Contractor Track-Kit Dollars Program which provides free Track-Kit IT related services credits for software enhancements specifically requested by the State. Fixed-price hourly rates for ancillary professional services will apply as defined in Schedule D – Pricing.

Contractor will track labor resource usage for new development after Phase III, if the work is to be performed on a time and material basis. The Contractor Accounting Team will provide the Contractor Project Manager

with a weekly labor report indicating all personnel and associated hours charged to the project which in turn be provided to the State's Service Manager.

The Contractor will provide "time to complete estimates" for each new development task. The Contractor Project Manager will use the "time to complete estimates" to forecast budget compliance and identify schedule risks.

All project related costs such as labor, contractors, variances and change orders will be tracked by the Contractor. The Contractor Project Manager will provide labor reports and budget updates to the State's Service Manger monthly, or as requested by the State.

5.1.6 F - Quality and Validation

The Contractor Quality Assurance Analyst will prepare the Specification Validation Plan based on the project requirements. The Final Specification Validation Plan will be used to verify that the final Solution delivered to the State meets the contract requirements prior to implementing Phase III.

5.1.7 G - Communications

The Contractor Project Manager is responsible for all communications with the State. The Contractor Project Manager will establish lines of communication with designated Contractor personnel and State personnel to ensure that the customer is kept informed of all relevant aspects of the project performance including quality, technical and contractual issues.

Ad-hoc communication will be conducted to address any topic or issues that would require immediate assistance or may not fall within the scope of the scheduled communication activities (Weekly Conference Call or Monthly Status Report).

As requested by the State, the Contractor Project Manager will both prepare and assist the State Project Manager in preparing special Reports and presentations related to the provision of the Solution for the State. The Contractor Project Manager and other Key Personnel will also provide or produce such reports or information as are requested by the State Project Manager.

Due to the Solution impacting hundreds of State organizations and thousands of State users, Contractor and the State will work jointly to communicate the status of the project via the internet on a site mutually agreed to by the parties. All communications to any user will be reviewed and approved by the State.

5.1.8 H - Risk Management

5.1.8.1 Risk Description

A risk is an unknown circumstance or event that, if it occurs, may have a positive or negative impact on the project.

The Contractor Project Manager will be responsible for developing a Risk Plan and continuously monitoring the risk assessments. The Risk Plan will be submitted to State for approval within twenty (20) business days after contract award. Once both parties have agreed to the format of the plan, it will become the standard to follow for the duration of the contract.

Risk Plan

The Contractor Project Manager will create a Risk Plan and process for the project in accordance with the State's methodology.

The Risk Plan will ensure that the information pertaining to the elements below are maintained and monitored:

- Risk description
- Risk priority which will be set by both parties
- Definition of the mitigation strategies for each identified risk

- Risk monitoring for maintaining risk status information

The risk management process will ensure that each identified risk is assessed monthly with the State and that all risk related information is updated accordingly.

Contractor will ensure that all risks for each phase of the project are identified and documented and we will be responsible for the mitigation and elimination of all risks assigned to us. Similarly, the State will be responsible for the mitigation and elimination of all risks assigned to them.

5.1.8.2 Risk Priority

Risks will be classified based on the probability and consequence of occurrence. Probability and consequence will be ranked as High, Medium and Low.

The Contractor Project Manager will establish 3x3 risk matrix to summarize the identified risks.

		Probability		
		High	Medium	Low
Consequence	High			
	Medium			
	Low			

5.1.8.3 Risk Contingency and Mitigation

The Contractor Project Manager will create detailed contingency plans for risks with a High-High or High-Medium rating. These contingency plans will detail recovery tasks necessary to quickly get the project back on track. Risks and contingency plans will be discussed with the Project Team on a weekly basis. Where possible, mitigation will be used to reduce the risk level.

Risks with a Medium-Medium or a High-Low rating will require high level contingency plans to ensure viability of recovery.

Risks with Medium-Low or Low-Low ratings will be monitored for change in status.

5.1.9 I - Issues Management

An issue or incident is an identified event that if not addressed may affect schedule, scope, quality, or budget.

Contractor will maintain issue logs for the Project.

While all issues are readily available to all stakeholders via the Customer Portal, the Contractor Project Manager will communicate all active issues to the State's Project Manager on an agreed-upon schedule, with email notifications and updates.

The issue log is updated by Contractor and contains the following minimum elements:

A. Description of issue

B. Issue identification date

C. Responsibility for resolving issue

D. Priority for issue resolution

E. Resources assigned responsibility for resolution

F. Resolution date

G. Resolution description

Note that additional fields can be easily added to the issue log if required.

The entire lifecycle of an issue can also be tracked using configurable workflows thus providing all stakeholders with real-time status information about all active issues.

The proposed escalation levels for issues are as follows, but can be modified on an agreed-upon set of values:

- Level 1 – Project Leads
- Level 2 – Project Managers
- Level 3 – Project Authority

5.1.10 J - Project Closeout

The Project Closeout definition will be when the State has granted Final Acceptance for Phase III.

The Project will enter the Support stage once the Testing and Acceptance milestone event for Phase II is reached and the State confirms Final Acceptance of the Solution in Phase III.

6. TRANSITION SERVICES

The Contractor must transition data formatted, at a minimum as XML, and within the expected timeframe specified in Section 24.3 Transition Responsibilities of the Contract Terms.

In addition, the Contractor will provide detailed documentation which will describe the purpose of each output as well as a full data dictionary and element definition. The outputs can then be used to transition\map the data into the new data structures. It is understood that the State will not assume any role or responsibilities for the extraction of the data and generation of the data files. Costs for Transition Services are listed on Schedule D – Pricing.

7. CONTRACTOR KEY PERSONNEL

Contractor Contract Administrator. Contractor Contract Administrator will (a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

Contractor
Name: Jocelyn Tremblay **Address:** 2255 St Laurent Blvd., Suite 206 Ottawa, ON K1G 4K3 **Phone:** 613-274-7822 x2000 **Email:** jocelyn.tremblay@stacsdna.com

Contractor Project Manager. Contractor Project Manager will serve as the primary contact with regard to services who will have the authority to act on behalf of the Contractor in matters pertaining to the implementation services.

Contractor
Name: Steven Gareau **Address:** 2255 St Laurent Blvd., Suite 206 Ottawa, ON K1G 4K3

Phone: 613-274-7822 x2008 **Email:** steven.gareau@stacsdna.com

Contractor Business Analyst Lead. Contractor Business Analyst Lead will serve as the primary contact to lead the requirements definition activities of the project in matters pertaining to the implementation services.

Contractor
Name: Ian Armstrong **Address:** 2255 St Laurent Blvd., Suite 206 **Phone:** 613-274-7822 x2014 **Email:** ian.armstrong@stacsdna.com

Contractor Development Lead. Contractor Development Lead will serve as the primary contact to lead development activities of the project in matters pertaining to the implementation services.

Contractor
Name: Olivier Diguer **Address:** 2255 St Laurent Blvd., Suite 206 **Phone:** 613-274-7822 x2013 **Email:** olivier.diguer@stacsdna.com

Contractor Service Manager. Contractor Service Manager will have the authority to act on behalf of Contractor in matters pertaining to the receipt and processing of Support Requests and the Support Services.

Contractor
Name: Kathleen Clarke **Address:** 2255 St Laurent Blvd., Suite 206 Ottawa, ON K1G 4K3 **Phone:** 613-274-7822 x2015 **Email:** kathleen.clarke@stacsdna.com

Contractor Security Officer. Contractor Security Officer will respond to State inquiries regarding the security of the Contractor's Solutions.

Contractor
Name: Steven Gareau **Address:** 2255 St Laurent Blvd., Suite 206 Ottawa, ON K1G 4K3 **Phone:** 613-274-7822 x2008 **Email:** steven.gareau@stacsdna.com

8. CONTRACTOR PERSONNEL REQUIREMENTS

Contractor must present certifications evidencing satisfactory Michigan State Police Background checks ICHAT and drug tests for all staff identified for assignment to this project.

In addition, proposed Contractor personnel will be required to complete and submit an RI-8 Fingerprint Card for the National Crime Information Center (NCIC) Finger Prints, if required by project.

Contractor will pay for all costs associated with ensuring their staff meets all requirements.

9. STATE RESOURCES/RESPONSIBILITIES

State Contract Administrator. The State Contract Administrator is the individual appointed by the State to (a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

State of Michigan
Name: Timothy Taylor **Address:** 525 W Allegan St, Lansing, MI 48929 **Phone:** 517-284-7006 **Email:** Taylort27@michigan.gov

State Project Manager. The State Project Manager will serve as the primary contact with regard to implementation Services who will have the authority to act on behalf of the State in approving Deliverables, and day to day activities.

State of Michigan
Name: Scott A. Cappel **Address:** 7150 Harris Drive, Dimondale, Michigan 48821 **Phone:** 517-897-2198 **Email:** cappels1@michigan.gov

Agency Business Owner. The Agency Business Owner will serve as the primary contact for the business area with regard to business advisement who will have the authority to act on behalf of the State in matters pertaining to the business Specifications.

State of Michigan
Name: Inspector John Bowen **Address:** Forensic Science Division Michigan State Police 7320 N. Canal Rd. Lansing, MI 48913 **Phone:** 517-512-5144 **Email:** BowenJ1@michigan.gov

State Technical Lead. The State Technical Lead will serve as the primary contact with regard to technical advisement who will have the authority to act on behalf of the State in matters pertaining to the technical Support Services.

State of Michigan
Name: Brian Piggott **Address:** 7150 Harris Drive, Dimondale, Michigan 48821 **Phone:** 517-243-0184 **Email:** piggottb@michigan.gov

Service Manager. The State Project Manager will serve as the primary contact with regard to Services who will have the authority to act on behalf of the State in matters pertaining to the Support Services, including the submission and processing of Support Requests.

State of Michigan

Name: TBD
Address: TBD
Phone: TBD
Email: TBD

10. PRICING

Contract costs are located within Schedule D – Pricing.
The State will be enrolled into the Contractor Track-Kit Dollars Program which provides free Track-Kit IT related services credits for software enhancements/customization that are requested by the State. Track-Kit Dollars are calculated based on 10% of the State's total annual fees. Track-Kit Dollars are not cumulative (year over year) and are not applicable against the State's annual fees. See Schedule D – Pricing for allotted annual service credits.
If Contractor reduces its prices for any of the software or services during the term of this Contract, the State shall have the immediate benefit of such lower prices for new purchases. Contractor shall send notice to the State's Contract Administrator with the reduced prices within fifteen (15) Business Days of the reduction taking effect.
The State does not pay for overtime or travel expenses.

11. INVOICING

Itemized invoices must include the contract number or purchase order number; contractor name, address, phone number; federal tax identification number; description of the Deliverables, and quantity ordered if applicable; date of delivery or installation, net invoice price for each item; total invoice price and be submitted to DTMB-Accounts-Payable@michigan.gov

12. ADDITONAL PRODUCTS AND SERVICES

The State reserves the right to purchase any additional products or services from the Contractor during the duration of the Contract.

Schedule A – Table 1

BUSINESS SPECIFICATIONS

Description of the Business Specifications Table

Column A: Business Specification number.

Column B: Business Specification description.

Column C: Contractor compliance with the business Specification.

- **Current Capability –** This capability must be available in the proposed system with no additional configuration or cost
- **Requires Configuration –** This capability must be met through vendor-supported changes to existing settings and application options as part of the initial implementation at no additional cost (e.g., setting naming conventions, creating user-defined fields).
- **Future Enhancement –** This capability must be a planned enhancement to the base software and will be available within the next 12 months at no additional cost.
- **Not Available –** This capability will not be available as part of initial implementation and a future enhancement is not planned.

  NOTE: Configuration is referred to as a modification to the system that must be completed by the Contractor prior to Go-Live but allows an IT or non-IT end user to maintain or modify thereafter (i.e. no source code or structural data model changes occurring). Any configuration changes must be forward-compatible with future releases and be fully supported by the Contractor without additional costs.

Column D: This column is for comments on how the Contractor will meet the business Specification.

A	B	C				D
Business Specification Number	**Business Specification**	**Current Capability**	**Requires Configuration**	**Future Enhancement**	**Not Available**	**Business Specification Comments**
1.0	The tracking system must be electronic and entry of information into the system must be web-based.	**X**				Track-Kit is a web-based system designed to be accessible from a desktop or mobile browser. Track-Kit is developed using Microsoft technologies and does not require any 3rd party plugins or additional libraries (Java, Flash, etc).
2.0	The tracking system must be able to integrate with MSP FSD's existing laboratory case management system (STaCS-CW)The tracking system must pull data from STaCS-CW to update the SAEK chain when a case is received by and/or completed by the laboratory.	**X**				Track-Kit is tightly integrated with the STACS-CW system and is updated in real-time when a SAK is received at the lab and when it has completed lab processing. Note: to enable the interface additional firewall ports and settings will need to be updated to support the communication between the two systems.
3.0	Portals must be provided for: ▪ Kit manufacturer and/or distributor (those entities may be separate or combined, at the State's discretion) ▪ Any accredited laboratory to whom the kits are sent for analysis ▪ Law enforcement ▪ Healthcare providers ▪ Prosecuting attorneys for each Michigan County ▪ Sexual assault victims/survivors	**X**				Track-Kit provides the following portal types, which tightly matches this business requirement: • Kit Distributor / Manufacturer Portal • Laboratory Portal • Law Enforcement Portal • Medical Facility Portal (Healthcare Providers) • Prosecutor Portal • Survivor Portal • Policy Center Portal (System Administration Center) • Compliance Oversight Portal

	▪ The Michigan Department of State Police (“MSP”), including the Michigan State Police – Forensic Science Division (“MSP-FSD”) ▪ The Michigan Domestic and Sexual Violence Prevention and Treatment Board (“The Board”)					There is also an Outsourcing Portal optionally available to track kits that are sent to private laboratories.
4.0	The proposed software must not make use of any specialized or proprietary hardware, devices and / or computers. NOTE: standard hand held bar code scanners are not considered specialized devices.	**X**				Track-Kit does not require any specialized or proprietary hardware, devices and / or computers. Track-Kit does support the use of standard hand held bar code scanners.
5.0	Provide secure user access through unique user ID and unique password for each user.	**X**				Each user of Track-Kit will have their own unique set of login credentials.
6.0	Provide Self-Help options – automated password resets	**X**				On the Login page Track-Kit users have the ability to request an email to reset their password.
7.0	Provide identification and tracking of kits via the manufacturer’s bar code number (this is also the kit number) pre-labeled on the kit.	**X**				Kits in the Track-Kit system may use the manufacturer barcodes. This is handled through the Distributor / Manufacturer portal, so that when kits are inserted into the Track-Kit workflow, they are assigned the right barcodes from the manufacturer.
8.0	Ability for users responsible for entering information into the system to enter kit ID by either scanning kit bar code or manually entering the kit number into system.	**X**				Track-Kit supports the ability to scan the bar code (kit Id) and if a scanner is not available or if the bar code is damaged or cannot be read the bar code can be manually entered. For manually entry bar codes the system can also be configured to require a

						second manual entry to valid the bar code was entered properly the first time.
9.0	Ability to (1) generate a unique password at the time a kit is entered into the system or at the time Healthcare logs the kit as having been used for evidence collection, for the victim/survivor to use to track their kit, (2) enter a pre-generated password for each victim, and (3) generate a voice message, e-mail or automatic text (to e-mail address or phone number designated by victim) sending link and instructions for accessing the system and for creating their own unique password.			**X**		Track-Kit currently supports the ability for the user recording the collection of the kit to enter a password that will be associated to the victim's user account. Sending an email, SMS, or a voice message to a survivor with login instructions would require the collection of this information into Track-Kit at the time of collection, which is a point up for discussion. Please see column D of point (31.) for more information.
10.0	Fields that provide the following information for data tracking and reporting purposes: 1. Date kit collected by Healthcare provider; 2. Date kit used for purpose other than sexual assault forensic medical examination and evidence collection ▪ Include a field for agency/entity using kit for this other purpose to indicate purpose 3. Whether kit has been released by victim to law enforcement; 4. Date on which Healthcare provider is no longer required to store the kit; ▪ This date would be, at minimum, one year after			**X**		Track-Kit currently collects the following fields at various steps through the workflow: • (1.) Kit Collection Date • (2.) Disposal Date o Disposal Reason (e.g. Training, Breakdown, etc.) • (3.) Whether the kit has been released by the victim to the Law Enforcement Agency • The Law Enforcement Agency (if applicable) that is assigned to this kit. • (4.) Disposal Date (date on which the kit may be disposed of by the Healthcare Provider) o This is based on a configurable minimum amount of time after the date of collection • (5.) The date on which the LEA was notified (if applicable)

	collection, but the system must be configurable so that Healthcare provider can set storage dates longer than one year if it chooses to do so. 5. Date Healthcare provider notifies law enforcement that kit has been released by victim to law enforcement; 6. Date law enforcement takes possession of kit from Healthcare provider or from another law enforcement agency; 7. Date law enforcement notifies law enforcement in different jurisdiction that it has a kit that belongs in that different jurisdiction; 8. Date law enforcement delivers kit to accredited laboratory for testing ▪ This field must be entered by law enforcement responsible for delivering the kit ▪ Entry date is contingent on law enforcement having entered a complaint number 9. Date that the laboratory receives the kit; 10. Date laboratory completes analysis of the kit;					• (6.) The date on which the LEA marks the kit as picked-up from the Healthcare Provider. • (7.) The date on which an LEA transfer was initiated • (9) .The date on which a kit was marked as received into the laboratory. • (10). Laboratory Analysis Complete Date • (11.) Date on which the LEA Picked up the completed kit from the Laboratory Modifications to Track-Kit will be required to accommodate the following field: • (8.) Currently, the Laboratory enters the date on which it was received from the LEA, not the other way around (9)

	11. Date on which law enforcement retrieves kit for storage after completion of laboratory analysis.					
11.0	Fields that require entry of the following information: 1. Law enforcement complaint number; 2. Laboratory number.	**X**				Track-Kit currently collects both the Laboratory Number and the Law Enforcement Complaint Number.
12.0	A field that allows, but does not require, law enforcement to enter its own unique property identifier.		**X**			Track-Kit supports the ability to create custom data fields (User Defined Fields). Read and write access to those fields can be controlled based on a per portal type basis. During initial system configuration, a UDF would be created for the Law Enforcement Property Identifier.
13.0	Time, date and user identity tracking whenever a user, except for a victim, accesses system. Access by a victim to the system will not be tracked by user identity.	**X**				Track-Kit collects a full audit trail of all access and modifications to any of the data in the system, as well as logging what actions a user undertakes. A User Activity Report is available to view the specific activities a given user performed. This functionality exempts the Survivor accounts.
14.0	Mandatory automatic notifications: 1. To law enforcement from Healthcare provider when kit has been released by victim. 2. To Healthcare provider storing unreleased kits, when the one-year (or longer) minimum storage date is approaching. The ability to configure these fields or add other fields that the Policy Center and local administrators	**X**				Track-Kit supports the ability for Policy Center users to define the notification message.

	determines are necessary or appropriate.					
15.0	A “hard stop” in the Healthcare provider initial entry section, so that if a victim has not signed a consent to release the kit to law enforcement, the Healthcare provider cannot click to automatically notify law enforcement that there is a kit to be picked up. This “hard stop” would be removed in the event that the victim later releases the kit to law enforcement.	**X**				In Track-Kit during the collection process, a "Released to Law Enforcement Agency" Yes / No selection is required. If "No" is selected, a LEA may not be specified and no Law Enforcement Agency will be notified of this new kit collection. This field can be changed to "Yes" at a later date if the survivor wishes so.
16.0	An optional automatic “hold” on victim access to tracking the location or lab submission status of the kit for a configurable time period (I.e. 48 hours) after the kit has been released to law enforcement. If no action is taken by law enforcement to continue the hold by flagging the kit per requirement 16.0 (below), the hold will expire. This option must be configurable by the State.			**X**		The system currently supports victim notifications; however, the system will need to be updated to support the ability to “hold” notifications.
17.0	The ongoing ability for law enforcement “flag” a kit at any time so that information about the location, lab submission status or storage of that kit is not accessible to the victim/survivor when law enforcement has determined that disclosure of that information to the victim will impede or compromise an ongoing investigation. 1. The system must send a configurable alert to the county prosecutor in that jurisdiction when a kit is flagged for this purpose.			**X**		Track-Kit supports a “flag” to hold conclusions generated in the lab from being automatically released to the survivor. This functionality will need to be enhanced to support the “flag” concept for location and status updates.

	2. The system must be configurable to allow notices/alerts to be sent to other appropriate parties.					
18.0	The generation/display of an advisory note that pops up in the system when victims log in and whose access to information about the location of their kits has been temporarily blocked by law enforcement. The language for this advisory note will be provided by the Policy Center and the system must allow configurability for changes in this language.			**X**		Track-Kit supports a survivor portal and will need to be enhanced to support the "flag" option as described in 17 and 18.
19.0	The ability to generate exception reports and for alerts to be automatically sent to the responsible agencies if timelines required by the Sexual Assault Evidence Kit Submission Act are not met for any particular kit. 1. The system must be configurable to allow each agency using the system to designate which person at the entity must receive these alerts. 2. These alerts cannot be turned off by the local agency, but the schedule, format, and frequency of delivery of these reports must be configurable by the Policy Center.	**X**				Track-Kit features a robust notification service to notify desired stakeholders when timeline thresholds set by the Sexual Assault Evidence Kit Submission Act are not respected. Each individual site may set one or more recipient(s) for individual notifications, so that only relevant stakeholders are sent notifications. The Policy Center configures the default format and delivery schedule for every notification types. Additionally, escalation levels are available for specific notifications so that notifications can be targeted towards the appropriate resource based on the criticality of the issue.
20.0	The system must be configured to allow agencies/entities using the system to configure and receive an alert warning them that a kit for which that agency or entity is	**X**				Notifications are available for kits that are approaching configured threshold settings for various steps through the workflow (e.g. Kit is approaching its Lab Submission Date, Kit has gone past its Lab Submission Date, etc.).

	responsible is approaching the deadline for retrieval or transfer 1. The timing of this alert, or blocking of this alert, must be configurable by the entity or agency.					In addition to notifications, relevant worklists have kits color coded based on their compliance to the configured time thresholds.
21.0	The ability for victims to securely verify their own account, obtain a new password in the event that they lose their password, and to opt-in to receive an automatic voice message, e-mail or text notification when the location, lab submission status, or storage of their kit changes.			**X**		This will need to be discussed in the JAD session as to SOM preferred approach. In the event that the survivor forget their password, if the survivor has provided an email address (optional field) for password reset purposes then a two factor authentication password reset process could be used. It has also been proposed that a separate card be provided which contains a unique serial number, the combination of the unique serial number and SAK barcode could be enough to reset the survivor password. It has also been proposed that Investigators could be given the ability to reset a survivor's password. In this context the survivor would call the investigator and once identified the investigator could reset the password.
22.0	Ability for the Policy Center to restrict user access to information in the system based on different permission levels (e.g., Hospital A has access to track and generate reports only on kits it used as part of a sexual assault medical forensic examination or that it has in inventory, Law Enforcement Agency X has access to track and generate reports on kits it has been notified have been released to it or which it has taken possession of or	**X**				Track-Kit features a strong role based access restriction system. The Policy Center is responsible for defining user access roles for each portal types. When a user is created, roles need to be associated to the user. The roles define to what functionality this user gains access to. Additionally, all of the portal sites only have access to kits for which they are responsible (e.g. LEA "A" will not be able

	delivered, State auditing agency has access to all information in statewide system, etc.).					to view the details of a kit that is assigned to LEA "B").
23.0	Ability for Policy Center to push or broadcast notices to some (based on role) or all users of the system.	**X**				Track-Kit supports the ability to define Bulletin Board Messages that will be displayed as a banner at the top of the home page of all of the portal types. When defining Bulletin Board Messages, the Policy Center may specify a target Portal Type and optionally a target portal site.
24.0	A user-friendly reporting function that allows users with report level permissions to easily generate reports that reflect their agency or organizational compliance with the Sexual Assault Evidence Kit Submission Act (configurable by agency, role, or organization).			**X**		Track-Kit features a reporting center for every portal type (excluding the Survivor Portal) with reports tailored to each stakeholders. During the JAD session we will review the needs of each individual stakeholders and modify existing / add new reports to best suit their needs. Additionally, a Kit Dynamic Search module is available to generate basic reports on kits in the system using dynamic search criteria. Users can save the search queries to re-use them later, as well as share them with other users.
25.0	The tracking system must have the ability to accommodate entry through a variety of mechanisms; for example, as web entry through computer or smartphone, or through scanning devices.	**X**				Track-Kit supports the ability to access kits for entry through various ways to accommodate as many users as possible. A handheld scanner may be used to scan the barcode of the kit. Alternatively, the kit barcode may be typed by hand into Track-Kit if no scanner is available. Finally, all the kits in the system can be reached by navigating the web interface

						and the various worklists, if manually typing the barcode is not possible.
26.0	The tracking system must allow Healthcare providers, law enforcement, and/or laboratories to enter their own information for an SAEK without regard to whether or not an entity that handled that kit previously has entered its own data for that kit. Laboratory entities must have the ability to enter the following data if not already entered into the system: Healthcare provider location where the kit was generated, the law enforcement jurisdiction that delivered the kit, and the law enforcement complaint number. An automatic alert must be (configurable and) delivered to those previous entities notifying them of the need to complete data entry.	**X**				Track-Kit supports the ability for any of the primary stakeholders (LEA, Lab) to receive a kit that may not already have had its collection recorded. In a case where a laboratory site receives a kit that has not had its collections details recorded by a healthcare staff, the receiving user would need to input some base information in regards to the provenance of the kit: • Healthcare Facility • Law Enforcement Agency • LEA Case Number (LEA Complaint Number) Additionally, the kit will be added to a Missing Information worklist for the previous agencies, and notifications are sent out. This is so that these agencies can go back and fill in this information that they have yet to record.
27.0	The system must be configured so that different persons and entities have different levels of access to information in the tracking system based on permissions granted by the Policy Center. These entities have access to enter data: • Healthcare; • Law enforcement; • Laboratory; • Kit manufacturer or distributor.	**X**				Track-Kit features a strong role based access restriction system. The Policy Center has the ability to define roles that will govern what functionality in the Track-Kit system a user gains access to. Roles are defined for each portal type.
28.0	These entities must have access to track kits: • Healthcare – to kits it collected (released or unreleased) or	**X**				The various portal types in Track-Kit have the ability to track kits along the natural workflow of a kit:

	that are in its own inventory of unused kits, or that it has transferred to any other entity for purposes other than sexual assault evidence collection; • Law enforcement – released kits that it has been notified of, retrieved, delivered, or stored; • Prosecutors – released kits that law enforcement has been notified of, retrieved, delivered, or stored in that prosecutor's county; • Michigan State Police Forensic Science Division – to track status of all released kits and to track inventory of all unused kits or kits that have been used for purposes other than administration of a sexual assault medical forensic examination; • Policy Center– to assist in troubleshooting; • Victims – to receive information about the location, lab submission status, and storage of sexual assault evidence that was gathered from them.					Healthcare users have access to kits that are: • In their agency's inventory • That have been collected (released to LEA or otherwise) by a user belonging to their agency Law Enforcement Agency Users have access to kits that are: • Collected, released, and assigned to their agency. • These kits may be in their inventory, at the laboratory or in storage Prosecutor users have access to kits that are: • Collected and released to LEA, and are part of the user's assigned Counties. Laboratory users have access to kits that are: • Collected and released to LEA • These kits may be In Transit to the laboratory, in the laboratory's possession, or in storage at the LEA following the completion of the lab process. The inventory of unused kits or kits that have been used for other purposes (e.g. broken down or used for training) can be viewed through the use of the Kit Dynamic Search. Policy Center users have access to all of the kits in the system. They have a global view of all the portal site's kits.

						Victim users only have read access to their kit—the one and only kit that is assigned to their user account.
29.0	The Michigan Domestic and Sexual Violence Prevention and Treatment Board must have access to local and statewide information in the system about released and unreleased kits, as well as unused kits or kits that have been used for purposes other than administration of a sexual assault medical forensic examination, in order to generate reports for policy and training purposes and/or to monitor agency compliance with the Sexual Assault Evidence Kit Submission Act.	**X**				Track-Kit features a Compliance Oversight portal This portal type exposes various dashboards and reports aimed at evaluating compliance of the relevant stakeholders to state legislation. Examples: Reports & dashboards on: • Unsubmitted kits • Stats for pickup time by LEAs from medical facilities • Delivery stats for kits from LEAs to laboratories
30.0	The system must be configurable by all users, except for victims, to allow users to generate unique reports from the information collected in the system based on user need.	**X**				Track-Kit features a reporting center for every portal type (excluding the Survivor Portal) with reports tailored to each stakeholders. Please see requirement (24.0) for more information.
31.0	Privacy of victim information in the tracking system must be protected by ensuring that personal identifying information about the victim, such as name, social security number, birth date, address, etc., is not allowed to be entered into the system by Healthcare providers, law enforcement, or laboratories. However, victims may choose to enter some of this information themselves as needed to manage their account or to set up user verification security, in which event the system must require as little of this personally identifying	**X**				By default Track-Kit does not collect any survivor personal identifying information. Once a survivor logs into the Track-Kit website, he/she may optionally opt-in into email and/or SMS notifications, for which we will collect an e-mail address and/or a phone number. This is entirely optional and is the only identifying identification about the survivor that is collected.

	information as possible in order to protect victim privacy (see requirement 31.0).					
32.0	The tracking system must be capable of allowing victims to electronically authorize the release of their kits to law enforcement, and that function must be able to be turned on or off by the state Policy Center. The system must be configurable by Policy Center to allow it to provide: • A method for verifying the identity of the victim authorizing release, that safeguards private victim information which may be needed as part of that verification process. • An information alert section, the content of which could be filled in by the Policy Center, to give the victim sufficient information to assure informed consent to the release. • Automatic notification of the release to (1) a responsible person at the Healthcare provider location, who can arrange for the kit to be located and made available for law enforcement retrieval, and (2) a responsible person at law enforcement so that law enforcement can retrieve the kit within the timelines required by statute. • A method for verifying the authorization of a victim that is compliant with state and federal privacy and security			**X**		A system setting (only accessible to the Policy Center) will be added that will govern the behavior of this feature. When the setting is turned on, a survivor that accesses the Track-Kit website will be able to authorize the release of their kit to Law Enforcement provided that information regarding the kit matches the following requirements: • The kit is marked as Unreleased in the Track-Kit system. • The kit has NOT been marked as a disposed in the Track-Kit system. • The user provides all of the required information in order for a staff member to confirm the survivor's identity. o Further details on this process will need to be obtained. Automatic notifications to relevant stakeholders at the Healthcare provider will be added so that they are made aware of newly released kits by survivors. Once the kit is found and an LEA is assigned, notifications will be sent to the LEA for pickup. More information regarding this feature will need to be gathered during the JAD session in regard to the verification of the victim's authorization, as well as in regard to the information alert section requested for the Policy Center.

	rules and regulations, including the Health Insurance Portability and Accountability Act (HIPAA) and its successor regulations.					
33.0	The tracking system must provide victims with unreleased kits the option to have a consent form, authorizing release of the kit, mailed to them at an address designated by them, for them to sign and mail to the Healthcare provider storing their kit.			**X**		Track-Kit tracks unreleased kits which may be released at a later date. Track-Kit does not currently support the mail option. To be discussed during the JAD session.
34.0	Bidder must demonstrate that persons staffing the help function have sufficient training and information to enable them to assist victims with access to the tracking system.	**X**				As per bidder response to question #27, the persons staffing the help function will have the same level of training regardless of the end user role.
35.0	The system must be configurable to allow the Policy Center to compile a county-by-county report of the data and responses and distribute to each county prosecutor the data for that county.			**X**		We will implement a county-by-county report that we will make available to prosecutors through the Prosecutor Portal. To be discussed during the JAD session.
36.0	The system must be configured in such a way as to allow the Policy Center to do the following: • Access the electronic tracking system and generate a draft report for each health care provider, law enforcement agency, and laboratory, which reflects: • the number of kits that were collected from health care providers and released to law enforcement that met the 24 hour notification deadline specified in the Sexual Assault Evidence Kit Submission Act			**X**		The Track-Kit system already collects and stores all of the data required to generate a report with all of the elements defined in this requirement. We will build a custom report into the Policy Center portal that will report on the compliance to the state legislation of the stakeholder for which it is generated. This report will be available to the individual sites of the Medical Facility, Law Enforcement Agency and Laboratory portals.

	and the number of kits that did not meet the deadline; • the number of released kits that were retrieved from health care providers (or from another law enforcement agency) by each law enforcement agency within the 14 day period specified in the Sexual Assault Evidence Kit Submission Act, and the number of released kits that were not retrieved within that 14 day period; • the number of kits that were delivered to an accredited laboratory within the 14 day period specified and the number of kits that were not delivered within that 14 day period; • the number of kits submitted to each accredited laboratory in which analysis was completed within the 90 day period recommended in the Sexual Assault Evidence Kit Submission Act and the number of kits in which analysis was not completed within that recommended time period; • the number of kits retrieved by law enforcement after analysis, and • the physical location as of the date of the draft report of all released kits collected by healthcare in that year; • Identification of agencies that have failed to enter required					This will be discussed in more details during the JAD session so that the final report tightly matches the expectation of the SOM in regards to this draft report.

	data as of the date of the report.					
37.0	As an option, the tracking system may include the following attributes: • Each draft report should be downloadable in pdf and the system should be configured to allow the auditing agency to e-mail the draft report specific to each entity to that entity's designated representative. • The tracking system adopted by the state should be configured in a way that would allow the Michigan Commission on Law Enforcement Standards to provide that system updated name and contact information when these commanding officers change at any entity. • The system should allow each audited entity to respond electronically to the draft report to either certify that the data reflected in that report is accurate, or that the data is not accurate, and provide an explanation for the discrepancy, including what the entity believes is the accurate data. • The system should provide a field in the draft report where each entity can briefly describe any challenges or barriers they have experienced in complying with Sexual Assault Evidence Kit Submission Act.			**X**		The Track-Kit system already provides the ability to export the generated reports to a plethora of formats, including PDF. The following functionality will need to be added to Track-Kit: • The ability for Track-Kit to email the generated Draft Report to a site's designated representative • The ability to define and manage the designated representative for individual sites We propose the following approach for the feedback loop from the representatives: • When the draft report is emailed to representatives, the email message will include a link to a form within Track-Kit. This form would allow them to respond to the draft report and certify whether that the data is accurate or not. Additionally, this form would allow them to submit any additional comments or explanations deemed necessary. • The initial draft report would be saved into Track-Kit along with the representative's response to it. • Members of the Board would be able to view each representative's draft reports along with the response that they would have submitted.

	• The system should allow the Board to merge the information from the draft reports and the responses from each entity into a final report.					• Using this information, the Board would be able to generate a final draft report that incorporate the responses from each representatives.

Exhibit A-Preliminary Project Plan

Status Indicator	Task Mode	Milestone	ID	% Complete	Task Name	Duration	Start	Finish	Predecessors	Resource Names
	Auto Scheduled	**No**	**1**	**0%**	**SAK Tracking System (Draft/Preliminary Implementation Plan)**	**148 days**	**Mon 1/22/18**	**Wed 8/15/18**		
	Auto Scheduled	Yes	2	0%	Contract Award	1 day	Mon 1/22/18	Mon 1/22/18		SOM
	Auto Scheduled	**No**	**3**	**0%**	**Phase I - Discovery, Analysis and Design**	**68 days**	**Mon 1/22/18**	**Wed 4/25/18**		
	Auto Scheduled	No	4	0%	Project Kick-off meeting	1 day	Mon 1/22/18	Mon 1/22/18		STACSDNA,SOM
	Auto Scheduled	No	5	0%	COTS Track-Kit Workflow Diagram	1 day	Tue 1/23/18	Tue 1/23/18	4	STACSDNA
	Auto Scheduled	**No**	**6**	**0%**	**Implementation Plan**	**4 days**	**Tue 1/23/18**	**Fri 1/26/18**		
	Auto Scheduled	No	7	0%	Generate and Submit Draft Implementation Plan	2 days	Tue 1/23/18	Wed 1/24/18	4	STACSDNA
	Auto Scheduled	No	8	0%	Review and Comment on Draft Implementation Plan	1 day	Thu 1/25/18	Thu 1/25/18	7	SOM
	Auto Scheduled	No	9	0%	Generate and Submit Preliminary Implementation Plan	1 day	Fri 1/26/18	Fri 1/26/18	8	STACSDNA
	Auto Scheduled	Yes	10	0%	Preliminary Project Implementation Sign-off	0 days	Fri 1/26/18	Fri 1/26/18	9	SOM
	Auto Scheduled	**No**	**11**	**0%**	**Gap Analysis**	**21 days**	**Mon 1/29/18**	**Mon 2/26/18**		
	Auto Scheduled	**No**	**12**	**0%**	**Conduct JAD Session**	**5 days**	**Mon 1/29/18**	**Fri 2/2/18**		**STACSDNA,SOM**

	Auto Scheduled	No	13	0%	Business Requirement Review	1 day	Mon 1/29/18	Mon 1/29/18	10	
	Auto Scheduled	No	14	0%	IT Requirement Review	1 day	Tue 1/30/18	Tue 1/30/18	13	
	Auto Scheduled	No	15	0%	Medical Facility Review	0.5 days	Wed 1/31/18	Wed 1/31/18	14	
	Auto Scheduled	No	16	0%	LEA Review	0.5 days	Wed 1/31/18	Wed 1/31/18	15	
	Auto Scheduled	No	17	0%	Lab Review	0.5 days	Thu 2/1/18	Thu 2/1/18	16	
	Auto Scheduled	No	18	0%	Policy Center	0.5 days	Thu 2/1/18	Thu 2/1/18	17	
	Auto Scheduled	No	19	0%	System Review	0.5 days	Fri 2/2/18	Fri 2/2/18	18	
	Auto Scheduled	No	20	0%	MI-Login Review	0.5 days	Fri 2/2/18	Fri 2/2/18	19	
	Auto Scheduled	**No**	**21**	**0%**	**Gap Analysis Generation**	**13 days**	**Mon 2/5/18**	**Wed 2/21/18**		
	Auto Scheduled	No	22	0%	Generate and Submit Draft 1 - Gap Analysis Report	5 days	Mon 2/5/18	Fri 2/9/18	20	STACSDNA
	Auto Scheduled	No	23	0%	Review Draft 1 - Gap Analysis Report	2 days	Mon 2/12/18	Tue 2/13/18	22	SOM
	Auto Scheduled	No	24	0%	Generate and Submit Draft 2 - Gap Analysis Report	2 days	Wed 2/14/18	Thu 2/15/18	23	STACSDNA
	Auto Scheduled	No	25	0%	Review Draft 2 - Gap Analysis Report	1 day	Fri 2/16/18	Fri 2/16/18	24	SOM
	Auto Scheduled	No	26	0%	Generate and Submit Final - GAP Analysis Report and Scope Assessment Report	1 day	Mon 2/19/18	Mon 2/19/18	25	STACSDNA,SOM
	Auto Scheduled	No	27	0%	Scope Agreement	2 days	Tue 2/20/18	Wed 2/21/18	26	STACSDNA,SOM
	Auto Scheduled	**No**	**28**	**0%**	**Final Scope Ratification**	**3 days**	**Thu 2/22/18**	**Mon 2/26/18**		
	Auto Scheduled	No	29	0%	Generate and Submit Final Scope Assessment Report	2 days	Thu 2/22/18	Fri 2/23/18	27	STACSDNA

	Auto Scheduled	No	30	0%	Generate and Submit Updated Project Plan	1 day	Mon 2/26/18	Mon 2/26/18	29	STACSDNA
	Auto Scheduled	Yes	31	0%	Final Gap Analysis	0 days	Mon 2/26/18	Mon 2/26/18	28	STACSDNA
	Auto Scheduled	Yes	32	0%	Final Scope and Assessment Report	0 days	Mon 2/26/18	Mon 2/26/18	28	STACSDNA
	Auto Scheduled	Yes	33	0%	Final Implementation Plan	0 days	Mon 2/26/18	Mon 2/26/18	28	STACSDNA
	Auto Scheduled	**No**	**34**	**0%**	**Customization and Testing**	**27 days**	**Tue 2/27/18**	**Wed 4/4/18**		
	Auto Scheduled	**No**	**35**	**0%**	**Sprint #1**	**18 days**	**Tue 2/27/18**	**Fri 3/23/18**		
	Auto Scheduled	**No**	**36**	**0%**	**System Requirements Definition - link to existing business and IT requirements**	**9 days**	**Tue 2/27/18**	**Fri 3/9/18**	**11**	
	Auto Scheduled	No	37	0%	Generate Detailed Specifications	4 days	Tue 2/27/18	Fri 3/2/18	28	STACSDNA
	Auto Scheduled	No	38	0%	Client Review	2 days	Mon 3/5/18	Tue 3/6/18	37	SOM
	Auto Scheduled	No	39	0%	Detailed Specification Update	1 day	Wed 3/7/18	Wed 3/7/18	38	STACSDNA
	Auto Scheduled	No	40	0%	Client Review	1 day	Thu 3/8/18	Thu 3/8/18	39	SOM
	Auto Scheduled	No	41	0%	Final Sprint Documentation	1 day	Fri 3/9/18	Fri 3/9/18	40	STACSDNA
	Auto Scheduled	Yes	42	0%	Sprint documentation sign-off	0 days	Fri 3/9/18	Fri 3/9/18	41	SOM
	Auto Scheduled	No	43	0%	Software Customization	11 days	Mon 3/5/18	Mon 3/19/18	37	STACSDNA
	Auto Scheduled	No	44	0%	Quality Assurance / Testing and Test Case development	7 days	Fri 3/9/18	Mon 3/19/18	40	STACSDNA
	Auto Scheduled	No	45	0%	Client Checkpoint / Review	1 day	Tue 3/20/18	Tue 3/20/18	44	STACSDNA,SOM
	Auto Scheduled	No	46	0%	Document Review	1 day	Wed 3/21/18	Wed 3/21/18	45	QA
	Auto Scheduled	No	47	0%	Scope Change Assessment	1 day	Thu 3/22/18	Thu 3/22/18	46	STACSDNA. SOM

	Auto Scheduled	Yes	48	0%	Sprint #1 Customization Release	0 days	Thu 3/22/18	Thu 3/22/18	47	STACSDNA
	Manually Scheduled	Yes	49	0%	Access Control and Audit; MiLogin Integration	0 days	Fri 3/23/18	Fri 3/23/18	47	STACSDNA
	Auto Scheduled	**No**	**50**	**0%**	**Sprint #2**	**18 days**	**Mon 3/12/18**	**Wed 4/4/18**		
	Auto Scheduled	**No**	**51**	**0%**	**System Requirements Definition - link to existing business and IT requirements**	**9 days**	**Mon 3/12/18**	**Thu 3/22/18**	**11**	
	Auto Scheduled	No	52	0%	Generate Detailed Specifications	4 days	Mon 3/12/18	Thu 3/15/18	41	STACSDNA
	Auto Scheduled	No	53	0%	Client Review	2 days	Fri 3/16/18	Mon 3/19/18	52	SOM
	Auto Scheduled	No	54	0%	Detailed Specification Update	1 day	Tue 3/20/18	Tue 3/20/18	53	STACSDNA
	Auto Scheduled	No	55	0%	Client Review	1 day	Wed 3/21/18	Wed 3/21/18	54	SOM
	Auto Scheduled	No	56	0%	Final Sprint Documentation	1 day	Thu 3/22/18	Thu 3/22/18	55	STACSDNA
	Auto Scheduled	Yes	57	0%	Sprint documentation sign-off	0 days	Thu 3/22/18	Thu 3/22/18	56	SOM
	Auto Scheduled	No	58	0%	Software Customization	11 days	Fri 3/16/18	Fri 3/30/18	52	STACSDNA
	Auto Scheduled	No	59	0%	Quality Assurance / Testing and Test Case development	7 days	Thu 3/22/18	Fri 3/30/18	55	STACSDNA
	Auto Scheduled	No	60	0%	Client Checkpoint / Review	1 day	Mon 4/2/18	Mon 4/2/18	59	STACSDNA,SOM
	Auto Scheduled	No	61	0%	Document Review	1 day	Tue 4/3/18	Tue 4/3/18	60	QA
	Auto Scheduled	No	62	0%	Scope Change Assessment	1 day	Wed 4/4/18	Wed 4/4/18	61	STACSDNA. SOM
	Auto Scheduled	Yes	63	0%	Sprint #2 Customization Release	0 days	Wed 4/4/18	Wed 4/4/18	62	STACSDNA
	Auto Scheduled	**No**	**64**	**0%**	**Documentation**	**30 days**	**Tue 2/27/18**	**Mon 4/9/18**		

	Auto Scheduled	No	65	0%	Generation of Policy Center Documentation	30 days	Tue 2/27/18	Mon 4/9/18	11	STACSDNA
	Auto Scheduled	Yes	66	0%	Policy Center Help Guide	0 days	Mon 4/9/18	Mon 4/9/18	65	STACSDNA
	Auto Scheduled	No	67	0%	Generation of End User Documentation	30 days	Tue 2/27/18	Mon 4/9/18	11	STACSDNA
	Auto Scheduled	Yes	68	0%	End User Documentation	0 days	Mon 4/9/18	Mon 4/9/18	67	STACSDNA
	Auto Scheduled	No	69	0%	Business Functional Specification Update	30 days	Tue 2/27/18	Mon 4/9/18	11	STACSDNA
	Auto Scheduled	Yes	70	0%	Interim Business Functional Specification	0 days	Mon 4/9/18	Mon 4/9/18	68	STACSDNA
	Auto Scheduled	**No**	**71**	**0%**	**Track-Kit System Setup / Configuration**	**24 days**	**Fri 3/23/18**	**Wed 4/25/18**		
	Auto Scheduled	**No**	**72**	**0%**	**Populate Portal Sites' Seed Data (Sites, Access Rights and Notification Setup and validation)**	**17 days**	**Fri 3/23/18**	**Mon 4/16/18**		
	Auto Scheduled	No	73	0%	Generate Info Gathering Template for Stakeholders	1 day	Fri 3/23/18	Fri 3/23/18	35	STACSDNA
	Auto Scheduled	No	74	0%	Submit Info Gathering Template to all Stakeholders	1 day	Mon 3/26/18	Mon 3/26/18	73	SOM
	Auto Scheduled	No	75	0%	Obtain Info from Pilot Site Stakeholders	10 days	Tue 3/27/18	Mon 4/9/18	74	SOM
	Auto Scheduled	No	76	0%	Populate Stakeholders Data in Track-Kit	5 days	Tue 4/10/18	Mon 4/16/18	75	STACSDNA
	Auto Scheduled	**No**	**77**	**0%**	**Solution Setup**	**14 days**	**Fri 3/23/18**	**Wed 4/11/18**		
	Auto Scheduled	No	78	0%	Environment Configuration	3 days	Fri 3/23/18	Tue 3/27/18	35	STACSDNA
	Auto Scheduled	No	79	0%	Code tables	2 days	Wed 3/28/18	Thu 3/29/18	78	STACSDNA

	Auto Scheduled	No	80	0%	Notification types	2 days	Wed 3/28/18	Thu 3/29/18	78	STACSDNA
	Auto Scheduled	No	81	0%	Spanish translations (as/if required) - for Survivor Portal	2 days	Wed 3/28/18	Thu 3/29/18	78	STACSDNA
	Auto Scheduled	No	82	0%	"Help" indicator descriptions (as/if required)	2 days	Wed 3/28/18	Thu 3/29/18	78	STACSDNA
	Auto Scheduled	No	83	0%	Roles and access rights for each portal	2 days	Fri 3/30/18	Mon 4/2/18	82	STACSDNA
	Auto Scheduled	No	84	0%	Policy Center (for Power Users) user accounts	2 days	Fri 3/30/18	Mon 4/2/18	82	STACSDNA
	Auto Scheduled	No	85	0%	SAK conclusions	5 days	Tue 4/3/18	Mon 4/9/18	84	STACSDNA
	Auto Scheduled	No	86	0%	User defined fields (as/if required)	5 days	Tue 4/3/18	Mon 4/9/18	84	STACSDNA
	Auto Scheduled	No	87	0%	System setting values	2 days	Tue 4/10/18	Wed 4/11/18	86	STACSDNA
	Auto Scheduled	**No**	**88**	**0%**	**Policy Center User Training (Train-the-Trainer)**	**10 days**	**Thu 4/5/18**	**Wed 4/18/18**		
	Auto Scheduled	No	89	0%	User Training Preparation	5 days	Thu 4/5/18	Wed 4/11/18	34	STACSDNA
	Auto Scheduled	No	90	0%	Training Session Execution	5 days	Thu 4/12/18	Wed 4/18/18	77	STACSDNA,SOM
	Auto Scheduled	**No**	**91**	**0%**	**Pre-Pilot User Validation**	**10 days**	**Thu 4/12/18**	**Wed 4/25/18**		
	Auto Scheduled	No	92	0%	User Acceptance Testing	5 days	Thu 4/12/18	Wed 4/18/18	77	STACSDNA,SOM
	Auto Scheduled	No	93	0%	Post User Acceptance Testing Stabilization	5 days	Thu 4/19/18	Wed 4/25/18	92	STACSDNA
	Auto Scheduled	Yes	94	0%	System Acceptance Deliverable	0 days	Wed 4/25/18	Wed 4/25/18	93	SOM
	Auto Scheduled	**No**	**95**	**0%**	**Phase II - Pilot Solution**	**16 days**	**Thu 4/26/18**	**Thu 5/17/18**		
	Manually Scheduled	Yes	96	0%	Final Pilot Approach/training plan	0 days	Fri 4/27/18	Fri 4/27/18	94	STACSDNA
	Auto Scheduled	No	97	0%	Pilot System Planning	1 day	Thu 4/26/18	Thu 4/26/18	94	STACSDNA,SOM

	Auto Scheduled	No	98	0%	Pilot User Training (one jurisdiction as identified by client)	2 days	Fri 4/27/18	Mon 4/30/18	97	STACSDNA,SOM
	Auto Scheduled	No	99	0%	Product use - Phase 1	5 days	Tue 5/1/18	Mon 5/7/18	98	STACSDNA,SOM
	Auto Scheduled	No	100	0%	Pilot project team checkpoint / status update	0.5 days	Tue 5/8/18	Tue 5/8/18	99	STACSDNA,SOM
	Auto Scheduled	No	101	0%	Product use - Phase 2	5 days	Tue 5/8/18	Mon 5/14/18	99	STACSDNA,SOM
	Auto Scheduled	No	102	0%	Pilot project team checkpoint / status update	0.5 days	Tue 5/15/18	Tue 5/15/18	101	STACSDNA,SOM
	Auto Scheduled	No	103	0%	Document pilot project results	0.5 days	Tue 5/15/18	Tue 5/15/18	102	STACSDNA,SOM
	Auto Scheduled	No	104	0%	Modify the system as needed based on Pilot results	2 days	Wed 5/16/18	Thu 5/17/18	103	STACSDNA,SOM
	Auto Scheduled	Yes	105	0%	Final Track-Kit System Deliverable	0 days	Thu 5/17/18	Thu 5/17/18	104	STACSDNA
	Auto Scheduled	Yes	106	0%	Final Business Functional Specification	0 days	Thu 5/17/18	Thu 5/17/18	104	STACSDNA
	Auto Scheduled	**No**	**107**	**0%**	**Phase III - Statewide Implementation and Roll-Out**	**64 days**	**Thu 5/17/18**	**Wed 8/15/18**		
	Auto Scheduled	Yes	108	0%	Final Roll-out Plan	0 days	Thu 5/17/18	Thu 5/17/18	95	STACSDNA/SOM
	Auto Scheduled	Yes	109	0%	End-User Support Fees and Track-Kit Licensing Fees begin	0 days	Fri 5/25/18	Fri 5/25/18	94FS+30 days	STACSDNA,SOM
	Auto Scheduled	Yes	110	0%	Final Acceptance	0 days	Wed 8/15/18	Wed 8/15/18	108FS+90 days	STACSDNA,SOM
	Auto Scheduled	**No**	**111**	**0%**	**Project Management Phase**	**148 days**	**Mon 1/22/18**	**Wed 8/15/18**		
	Auto Scheduled	Yes	112	0%	Weekly Meeting	0 days	Mon 1/22/18	Mon 1/22/18	4SS	STACSDNA,SOM
	Auto Scheduled	Yes	113	0%	Monthly Status Reports	0 days	Wed 8/15/18	Wed 8/15/18	107FF	STACSDNA,SOM

SCHEDULE B
Service Level Agreement

1. Definitions. For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this **Section 1** shall have the respective meanings given to them in the Contract.

"**Actual Uptime**" means the total minutes in the Service Period that the Hosted Services are Available.

"**Authorized Users**" means all Persons authorized by the State to access and use the Services through the State's account under the Contract.

"**Availability**" has the meaning set forth in **Section 4(a)**.

"**Availability Requirement**" has the meaning set forth in **Section 4(a)**.

"**Available**" has the meaning set forth in **Section 4(a)**.

"**Business Day**" means a day other than a Saturday, Sunday or State Holiday.

"**Contractor Service Manager**" has the meaning set forth in **Section 3.1**.

"**Corrective Action Plan**" has the meaning set forth in **Section 5.6**.

"**Critical Service Error**" has the meaning set forth in **Section 5.4(a)**.

"**Exceptions**" has the meaning set forth in **Section 4.2**.

"**Force Majeure Event**" has the meaning set forth in **Section 6.1**.

"**High Service Error**" has the meaning set forth in **Section 5.4(a)**.

"**Hosted Services**" has the meaning set forth in **Section 2.1(a)**.

"**Low Service Error**" has the meaning set forth in **Section 5.4(a)**.

"**Medium Service Error**" has the meaning set forth in **Section 5.4(a)**.

"**Resolve**" has the meaning set forth in **Section 5.4(b)**.

"**Scheduled Downtime**" has the meaning set forth in **Section 4.3**.

"**Scheduled Uptime**" means the total minutes in the Service Period.

"**Service Availability Credits**" has the meaning set forth in **Section 4.6(a)**.

"**Service Error**" means any failure caused by Contractor or any of its Permitted Subcontractors or Affiliates of any Hosted Service to be Available or otherwise perform in accordance with this Schedule.

"**Service Level Credits**" has the meaning set forth in **Section 5.5**.

"**Service Level Failure**" means a failure to perform the Software Support Services fully in compliance with the Support Service Level Requirements.

"**Service Period**" has the meaning set forth in **Section 4(a)**.

"**Services**" has the meaning set forth in **Section 2.1**.

"**Software**" has the meaning set forth in the Contract.

"**Software Support Services**" has the meaning set forth in **Section 5**.

"**State**" means the State of Michigan.

"**State Service Manager**" has the meaning set forth in **Section 3.2**.

"**State Systems**" means the information technology infrastructure, including the computers, software, databases, electronic systems (including database management systems) and networks, of the State or any of its designees.

"**Support Request**" has the meaning set forth in **Section 5.4(a)**.

"**Support Service Level Requirements**" has the meaning set forth in **Section 5.4**.

"**Term**" has the meaning set forth in the Contract.

2. Services.

2.1 Services. Throughout the Term, Contractor will, in accordance with all terms and conditions set forth in the Contract and this Schedule, provide to the State and its Authorized Users the following services ("**Services**"):

(a) the hosting, management and operation of the Software and other services for remote electronic access and use by the State and its Authorized Users ("**Hosted Services**");

(b) the Software Support Services set forth in **Section 5** of this Schedule;

3. Personnel

3.1 Contractor Personnel for the Hosted Services. Contractor will appoint a Contractor employee to serve as a primary contact with respect to the Services who will have the authority to act on behalf of Contractor in matters pertaining to the receipt and processing of Support

Requests and the Software Support Services (the "**Contractor Service Manager**"). The Contractor Service Manager will be considered Key Personnel under the Contract.

3.2 State Service Manager for the Hosted Services. The State will appoint and, in its reasonable discretion, replace, a State employee to serve as the primary contact with respect to the Services who will have the authority to act on behalf of the State in matters pertaining to the Software Support Services, including the submission and processing of Support Requests (the "**State Service Manager**").

4. Service Availability and Service Availability Credits.

(a) Availability Requirement. Contractor will make the Hosted Services Available, as measured over the course of each calendar month during the Term and any additional periods during which Contractor does or is required to perform any Hosted Services (each such calendar month, a "**Service Period**"), at least 99.0% of the time, excluding only the time the Hosted Services are not Available solely as a result of one or more Exceptions (the "**Availability Requirement**"). "**Available**" means the Hosted Services are available and operable for access and use by the State and its Authorized Users over the Internet in material conformity with the Contract. "**Availability**" has a correlative meaning. The Hosted Services are not considered Available in the event of a material performance degradation or inoperability of the Hosted Services, in whole or in part. The Availability Requirement will be calculated for the Service Period as follows: (Actual Uptime – Total Minutes in Service Period Hosted Services are not Available Due to an Exception) ÷ (Scheduled Uptime – Total Minutes in Service Period Hosted Services are not Available Due to an Exception) x 100 = Availability.

4.2 Exceptions. No period of Hosted Service degradation or inoperability will be included in calculating Availability to the extent that such downtime or degradation is due to any of the following ("**Exceptions**"):

(a) failures of the State's or its Authorized Users' internet connectivity;

(b) a Force Majeure Event that simultaneously and materially impairs the ability of the Contractor to deliver the Hosted Services from all of its operating and backup sites; or

(c) Scheduled Downtime as set forth in **Section 4.3**.

4.3 Scheduled Downtime. Contractor must notify the State at least five (5) days in advance of all scheduled outages of the Hosted Services in whole or in part ("**Scheduled Downtime**"). All such scheduled outages will: (a) last no longer than five (5) hours; (b) be scheduled between the hours of 12:00 a.m. and 5:00 a.m., Eastern Time; and (c) occur no more frequently than once per week; provided that Contractor may request the State to approve extensions of Scheduled Downtime above five (5) hours, and such approval by the State may not be unreasonably withheld or delayed.

4.4 Software Response Time. Software response time, defined as the interval from the time the end user sends a transaction to the time a visual confirmation of transaction completion is received, is as follows:

(a) average time to generate a page load may not exceed 2 seconds 98% of the time

(b) average time to view a worklist screen should not exceed 3 seconds 90% of the time based on default filters; provided, however, that if Authorized Users do not use default filters and instead adjust filters to retrieve large amounts of data, Response Time will be negatively affected. .

The State understands that factors beyond Contractor's control may negatively affect Response Time (such as internet speed or connection, browser settings, and the amount of data requested by an Authorized User in one transaction). Unacceptable response times due to factors within Contractor's control shall be considered to make the Software unavailable and will count against the Availability Requirement.

4.5 Service Availability Reports. Within thirty (30) days after the end of each Service Period, Contractor will provide to the State a report describing the Availability and other performance of the Hosted Services during that calendar month as compared to the Availability Requirement. The report must be in electronic or such other form as the State may approve in writing and shall include, at a minimum: (a) the actual performance of the Hosted Services relative to the Availability Requirement; and (b) if Hosted Service performance has failed in any respect to meet or exceed the Availability Requirement during the reporting period, a description in sufficient detail to inform the State of the cause of such failure and the corrective actions the Contractor has taken and will take to ensure that the Availability Requirement are fully met.

4.6 Remedies for Service Availability Failures.

(a) If the actual Availability of the Hosted Services is less than the Availability Requirement for any Service Period, such failure will constitute a Service Error for which Contractor will issue to the State the following credits on the fees payable for Hosted Services provided during the Service Period ("**Service Availability Credits**"):

Availability	**Credit of Fees**
≥99.0%	None
<99.0% but ≥95.0%	20%
<95.0% but ≥90.0%	50%
<90.0%	100%

(b) Any Service Availability Credits due under this **Section 4.6** will be applied in accordance with payment terms of the Contract.

(c) If the actual Availability of the Hosted Services is less than the Availability Requirement in any two (2) of four (4) consecutive Service Periods, then, in addition to all other remedies available to the State, the State may terminate the Contract on written notice to Contractor with no liability, obligation or penalty to the State by reason of such termination.

5. Support and Maintenance Services. Contractor will provide Hosted Service maintenance and support services (collectively, "**Software Support Services**") in accordance with the provisions of this **Section 5**. The Software Support Services are included in the Services, and Contractor may not assess any additional fees, costs or charges for such Software Support Services.

5.1 Support Service Responsibilities. Contractor will:

(a) correct all Service Errors in accordance with the Support Service Level Requirements, including by providing defect repair, programming corrections and remedial programming;

(b) unless otherwise provided in the applicable Statement of Work, provide unlimited telephone support Monday through Friday from 8:00 a.m. to 5 p.m., except on State Holidays;

(c) provide the ability to submit unlimited online support requests 24 hours a day, seven days a week;

(d) provide online access to technical support bulletins and other user support information and forums, to the full extent Contractor makes such resources available to its other customers; and

(e) respond to and Resolve Support Requests as specified in this **Section 5**.

5.2 Service Monitoring and Management. Contractor will continuously monitor and manage the Hosted Services to optimize Availability that meets or exceeds the Availability Requirement. Such monitoring and management includes:

(a) proactively monitoring on a twenty-four (24) hour by seven (7) day basis all Hosted Service functions, servers, firewall and other components of Hosted Service security;

(b) if such monitoring identifies, or Contractor otherwise becomes aware of, any circumstance that is reasonably likely to threaten the Availability of the Hosted Service, taking all necessary and reasonable remedial measures to promptly eliminate such threat and ensure full Availability; and

(c) if Contractor receives knowledge that the Hosted Service or any Hosted Service function or component is not Available (including by written notice from the State pursuant to the procedures set forth herein):

(i) confirming (or disconfirming) the outage by a direct check of the associated facility or facilities;

(ii) if Contractor's facility check in accordance with clause (i) above confirms a Hosted Service outage in whole or in part: (A) notifying the State in writing pursuant to the procedures set forth herein that an outage has occurred, providing such details as may be available, including a Contractor trouble ticket number, if appropriate, and time of outage; and (B) working all problems causing and caused by the outage until they are Resolved as Critical Service Errors in accordance with the Support Request Classification set forth in **Section 5.4**, or, if determined to be an internet provider problem, open a trouble ticket with the internet provider; and

(iii) notifying the State that Contractor has fully corrected the outage and any related problems, along with any pertinent findings or action taken to close the trouble ticket.

5.3 Service Maintenance. Contractor will continuously maintain the Hosted Services to optimize Availability that meets or exceeds the Availability Requirement. Such maintenance services include providing to the State and its Authorized Users:

(a) all updates, bug fixes, enhancements, new releases, new versions and other improvements to the Hosted Services, including the Software, that Contractor provides at no additional charge to its other similarly situated customers; and

(b) all such services and repairs as are required to maintain the Hosted Services or are ancillary, necessary or otherwise related to the State's or its Authorized Users' access to or use of the Hosted Services, so that the Hosted Services operate properly in accordance with the Contract and this Schedule.

5.4 Support Service Level Requirements. Contractor will correct all Service Errors and respond to and Resolve all Support Requests in accordance with the required times and other terms and conditions set forth in this **Section 5.4** ("**Support Service Level Requirements**"), and the Contract.

(a) Support Requests. The State will classify its requests for Service Error corrections in accordance with the descriptions set forth in the chart below (each a "**Support Request**"). The State Service Manager will notify Contractor of Support Requests by email, telephone or such other means as the parties may hereafter agree to in writing.

Support Request Classification	Description: Any Service Error Comprising or Causing any of the Following Events or Effects
Critical Service Error	• Issue affecting entire system or single critical production function;

	• System down or operating in materially degraded state; • Data integrity at risk; or • Widespread access interruptions.
High Service Error	• Primary component failure that materially impairs its performance; or • Data entry or access is materially impaired on a limited basis.
Medium Service Error	• Hosted Service is operating with minor issues that can be addressed with a work around.
Low Service Error	• Request for assistance, information, or services that are routine in nature.

(b) Response and Resolution Time Service Levels. Response and Resolution times will be measured from the time Contractor receives a Support Request until the respective times Contractor has (i) responded to, in the case of response time and (ii) Resolved such Support Request, in the case of Resolution time. "**Resolve**" (including "**Resolved**", "**Resolution**" and correlative capitalized terms) means that, as to any Service Error, Contractor has provided the State the corresponding Service Error correction and the State has confirmed such correction and its acceptance thereof. Contractor will respond to and Resolve all Service Errors within the following times based on the severity of the Service Error:

Support Request Classification	Service Level Metric (Required Response Time)	Service Level Metric (Required Resolution Time)	Service Level Credits (For Failure to Respond to any Support Request Within the Corresponding Response Time)	Service Level Credits (For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)

Critical Service Error	One (1) hour	Four (4) hours	Five percent (5%) of the Fees for the month in which the initial Service Level Failure begins and five percent (5%) of such monthly Fees for each additional hour or portion thereof that the corresponding Service Error is not responded to within the required response time.	Five percent (5%) of the Fees for the month in which the initial Service Level Failure begins and five percent (5%) of such monthly Fees for each block of 4 hours or portion thereof that the corresponding Service Error remains un-Resolved.
High Service Error	One (1) hour	Four (4) hours	Three percent (3%) of the Fees for the month in which the initial Service Level Failure begins and three percent (3%) of such monthly Fees for each additional hour or portion thereof that the corresponding Service Error is not responded to within the required response time.	Three percent (3%) of the Fees for the month in which the initial Service Level Failure begins and three percent (3%) of such monthly Fees each block of 4 hours or portion thereof that the corresponding Service Error remains un-Resolved.
Medium Service Error	Three (3) hours	Two (2) Business Days	N/A	N/A
Low Service Error	Three (3) hours	Five (5) Business Days	N/A	N/A

(c) Escalation. With respect to any Critical Service Error Support Request, until such Support Request is Resolved, Contractor will escalate that Support Request within sixty (60) minutes of the receipt of such Support Request by the appropriate Contractor support personnel, including, as applicable, the Contractor Service Manager and Contractor's management or engineering personnel, as appropriate.

5.5 Support Service Level Credits. Failure to achieve any of the Support Service Level Requirements for Critical and High Service Errors will constitute a Service Level Failure for which Contractor will issue to the State the corresponding service credits set forth in **Section 5.4(b)** ("**Service Level Credits**") in accordance with payment terms set forth in the Contract.

5.6 Corrective Action Plan. If two or more Critical Service Errors occur in any thirty (30) day period during (a) the Term or (b) any additional periods during which Contractor does or is required to perform any Hosted Services, Contractor will promptly investigate the root causes of these Service Errors and provide to the State within five (5) Business Days of its receipt of notice of the second such Support Request an analysis of such root causes and a proposed written corrective action plan for the State's review, comment and approval, which, subject to and upon the State's written approval, shall be a part of, and by this reference is incorporated in, the Contract as the parties' corrective action plan (the "**Corrective Action Plan**"). The State will review and comment the Corrective Action Plan within five (5) Business Days of its receipt from Contractor. The Corrective Action Plan must include, at a minimum: (a) Contractor's commitment to the State to devote the appropriate time, skilled personnel, systems support and equipment and other resources necessary to Resolve and prevent any further occurrences of the Service Errors giving rise to such Support Requests; (b) a strategy for developing any programming, software updates, fixes, patches, etc. necessary to remedy, and prevent any further occurrences of, such Service Errors; and (c) time frames for implementing the Corrective Action Plan. There will be no additional charge for Contractor's preparation or implementation of the Corrective Action Plan in the time frames and manner set forth therein.

6. Force Majeure.

6.1 Force Majeure Events. Subject to **Section 6.3**, neither party will be liable or responsible to the other party, or be deemed to have defaulted under or breached the Contract, for any failure or delay in fulfilling or performing any term hereof, when and to the extent such failure or delay is caused by: acts of God, flood, fire or explosion, war, terrorism, invasion, riot or other civil unrest, embargoes or blockades in effect on or after the date of the Contract, national or regional emergency, or any passage of law or governmental order, rule, regulation or direction, or any action taken by a governmental or public authority, including imposing an embargo, export or import restriction, quota or other restriction or prohibition (each of the foregoing, a "**Force Majeure Event**"), in each case provided that: (a) such event is outside the reasonable control of the affected party; (b) the affected party gives prompt written notice to the other party, stating the period of time the occurrence is expected to continue; (c) the affected party uses diligent efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

6.2 State Performance; Termination. In the event of a Force Majeure Event affecting Contractor's performance under the Contract, the State may suspend its performance hereunder until such time as Contractor resumes performance. The State may terminate the Contract by written notice to Contractor if a Force Majeure Event affecting Contractor's performance hereunder continues substantially uninterrupted for a period of five (5) Business Days or more. Unless the State terminates the Contract pursuant to the preceding sentence, any date specifically designated for Contractor's performance under the Contract will automatically be extended for a period up to the duration of the Force Majeure Event.

6.3 Exclusions; Non-suspended Obligations. Notwithstanding the foregoing or any other provisions of the Contract or this Schedule:

(a) in no event will any of the following be considered a Force Majeure Event:

(i) shutdowns, disruptions or malfunctions of Contractor Systems or any of Contractor's telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to the Contractor Systems; or

the delay or failure of any Contractor Personnel to perform any obligation of Contractor hereunder unless such delay or failure to perform is itself by reason of a Force Majeure Event.

SCHEDULE D-Pricing

SAEK Schedule D – Pricing						
	Contract Cost (Dollars)					
	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Description						
Project Milestone/Deliverables:						
Phase I - Discovery, Analysis and Design Final Gap Analysis Final Scope and Assessment Report	$9,980.85					$9,980.85
Phase I - Discovery, Analysis and Design Final Implementation Plan	$6,653.90					$6,653.90
Phase I - Discovery, Analysis and Design Access Control and Audit; MiLogin Integration	$6,802.00					$6,802.00
Phase I - Discovery, Analysis and Design System Acceptance	$29,923.40					$29,923.40
Phase II - Pilot Solution Final Pilot Approach Plan Final Training Plan Final Pilot Track-Kit System	$6,653.90					$6,653.90
Phase II - Pilot Solution Final Specification Validation Plan	$3,326.95					$3,326.95
Phase III – Statewide Implementation Rollout Final Roll-out Plan 90-day warranty Final Acceptance	$10,000.00					$10,000.00
Discount Included (See Note 1 below)						

Implementation Total	$73,341.00					**$73,341.00**
Licensing (Fees) - (See Note 2 and Note 3 below)	$200,000.00	$204,000.00	$208,080.00	$212,241.60	$216,486.43	**$1,040,808.03**
End-User Support (Fees) - (See Note 4 below)	$473,200.00	$482,664.00	$492,317.00	$502,164.00	$512,207.00	**$2,462,552.00**
TOTAL	**$746,541.00**	**$686,664.00**	**$700,397.00**	**$714,405.60**	**$728,693.43**	**$3,576,701.03**

Note 1 (Discount):

The breakdown of the discounted amounts for the above implementation deliverables will be as follows:

Deliverable	Original Cost	Disc. Cost
Final Gap Analysis / Final Scope and Assessment Report	$19,961.70	$9,980.85
Final Implementation Plan	$13,307.80	$6,653.90
Access Control and Audit; MiLogin Integration	$13,604.00	$6,802.00
System Acceptance	$39,846.80	$29,923.40
Final Pilot Approach Plan/Final Training Plan/Final Pilot Track-Kit System	$13,307.80	$6,653.90
Final Specification Validation Plan	$6,653.90	$3,326.95
Final Roll-out Plan/90-day warranty/Final Acceptance	$39,923.40	$10,000.00
Total - Project Deliverables	**$146,605.40**	**$73,341.00**

Note 2 (Licensing - Track-Kit Dollars Program):

State will be entitled to the following Track-Kit Dollars (free credits):

Year 1:	$20,000.00
Year 2:	$20,400.00
Year 3:	$20,808.00
Year 4:	$21,224.16
Year 5:	$21,648.64

$(104,080.80)

Note 3 (Licensing –Monthly Fees):

The Track-Kit Licensing fees (excluding the End-User Support Services) will be invoiced on a monthly basis as follows beginning upon 30 days after Phase I - Discovery, Analysis and Design System Acceptance.

Year	Monthly Fee	Months	Annual Cost
Year 1:	$16,666.67	12	$200,000.00
Year 2:	$17,000.00	12	$204,000.00
Year 3:	$17,340.00	12	$208,080.00
Year 4:	$17,686.80	12	$212,241.60
Year 5:	$18,040.54	12	$216,486.43
		Total 5-year Cost	$1,040,808.03

Note 4 (End-User Support Options):

The State will initially require Option 4. See Schedule - A Statement of Work Section 4.3.2 Support for details. The End-User Support will be invoiced on a monthly basis as follows beginning upon 30 days after Phase I - Discovery, Analysis and Design System Acceptance.

Online Chat Support				
Year 1	**Year 2**	**Year 3**	**Year 4**	**Year 5**

Option 1 - 8 a.m. – 5 p.m. Monday through Friday	$67,200	$68,544	$69,915	$71,313	$72,739	**$349,711.00**
Option 2 - Extended business hours Monday through Friday (6h00-21h00)	$134,400	$137,088	$139,830	$142,626	$145,479	**$699,423.00**
Option 3 - Extended business hours - 365 days a year (6h00-21h00)	$224,000	$228,480	$233,050	$237,711	$242,465	**$1,165,705.00**
Option 4 - 24 hours a day, 365 days a year	$378,560	$386,131	$393,854	$401,731	$409,766	**$1,970,041.00**

	Online Chat and Phone Support					
	Year 1	**Year 2**	**Year 3**	**Year 4**	**Year 5**	
Option 1 - 8 a.m. – 5 p.m. Monday through Friday	$84,000	$85,680	$87,394	$89,141	$90,924	**$437,139.00**
Option 2 - Extended business hours Monday through Friday (6h00-21h00)	$168,000	$171,360	$174,787	$178,283	$181,849	**$874,279.00**
Option 3 - Extended business hours - 365 days a year (6h00-21h00)	$280,000	$285,600	$291,312	$297,138	$303,081	**$1,457,131.00**
Option 4 - 24 hours a day, 365 days a year	$473,200	$482,664	$492,317	$502,164	$512,207	**$2,462,552.00**

Fixed-price hourly rates for ancillary professional services (same rates for on-site and remote services)

Role	**2017**	**2018**	**2019**	**2020**	**2021**
Project Manager	$225.00	$229.50	$234.00	$238.50	$243.50
Business/System Analyst	$173.50	$177.00	$180.50	$184.50	$188.00
Software Developer	$179.00	$182.50	$186.00	$190.00	$193.50
QA Analyst	$168.50	$172.00	$175.50	$179.00	$182.50
Infrastructure Engineer	$168.50	$172.00	$175.50	$179.00	$182.50
Technical Writer	$168.50	$172.00	$175.50	$179.00	$182.50

Trainer	$168.50	$172.00	$175.50	$179.00	$182.50

Fixed-price fees schedule (per individual training session) for ongoing training beyond the initial Implementation Services (webinar-based training)

- Fees include:
  - Coordination and scheduling of training sessions
  - Access to the webinar platform
  - Actual training delivery for up to 25 participants per training session
- Fees are based on the above "Trainer" hourly rate

User Type	2017	2018	2019	2020	2021
Policy Center	$1,348.00	$1,374.96	$1,402.46	$1,430.51	$1,459.12
Medical Facility	$842.50	$859.35	$876.54	$894.07	$911.95
Law Enforcement Agency	$1,516.50	$1,546.83	$1,577.77	$1,609.32	$1,641.51
Laboratory	$1,179.50	$1,203.09	$1,227.15	$1,251.69	$1,276.73
Distributor	$842.50	$859.35	$876.54	$894.07	$911.95
Prosecutor	$505.50	$515.61	$525.92	$536.44	$547.17
Private Laboratory	$674.00	$687.48	$701.23	$715.25	$729.56

Transition Services

Upon termination or expiration of the agreement STACS DNA will provide data migration support to SOM.
The estimated effort for performing this task is 40 hours.
The corresponding fees will be based on our "Software developer" hourly rate for the year the services will be required

	2017	2018	2019	2020	2021
One-time fee - 40 hours	$7,160.00	$7,300.00	$7,440.00	$7,600.00	$7,740.00

Schedule E-Disaster Recovery Plan-Confidential

SCHEDULE F
Data Security Terms

1. Definitions. For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this **Section 1** shall have the respective meanings given to them in the Contract.

"**Contractor Security Officer**" has the meaning set forth in **Section 2** of this Schedule.

"**Contractor Systems**" has the meaning set forth in **Section 5** of this Schedule.

"**FedRAMP**" means the Federal Risk and Authorization Program, which is a federally approved risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

"**NIST**" means the National Institute of Standards and Technology.

2. Contractor will appoint a Contractor employee to respond to the State's inquiries regarding the security of the Contractor Systems who has sufficient knowledge of the security of the Contractor Systems and the authority to act on behalf of Contractor in matters pertaining thereto ("**Contractor Security Officer**"). The Contractor Security Officer will be considered Key Personnel under the Contract.

3. Protection of the State's Confidential Information. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will:

3.1 maintain FedRAMP certification for the Hosted Services throughout the Term;

3.2 ensure that the Software is securely hosted, supported, administered, and accessed in a data center that resides in the continental United States, and minimally meets Uptime Institute Tier 3 standards (www.uptimeinstitute.com), or its equivalent;

3.3 maintain and enforce an information security program including safety and physical and technical security policies and procedures with respect to its Processing of the State's Confidential Information that comply with the requirements of the State's data security policies as set forth in the Contract**,** and must, at a minimum, remain compliant with the NIST Special Publication 800.53 (most recent version) MOD Controls;

3.4 provide technical and organizational safeguards against accidental, unlawful or unauthorized access to or use, destruction, loss, alteration, disclosure, transfer, commingling or processing of such information that ensure a level of security appropriate to the risks presented by the processing of the State's Confidential Information and the nature of such Confidential Information, consistent with best industry practice and standards;

3.5 take all reasonable measures to:

(a) secure and defend all locations, equipment, systems and other materials and facilities employed in connection with the Services against “hackers” and others who may seek, without authorization, to disrupt, damage, modify, access or otherwise use Contractor Systems or the information found therein; and

(b) prevent (i) the State and its Authorized Users from having access to the data of other customers or such other customer’s users of the Services; (ii) the State’s Confidential Information from being commingled with or contaminated by the data of other customers or their users of the Services; and (iii) unauthorized access to any of the State’s Confidential Information;

3.6 State Data must be encrypted in transit and at rest using AES 256bit or higher encryption;

3.7 the Hosted Services must support Identity Federation/Single Sign-on (SSO) capabilities using SAML or comparable mechanisms; and

3.8 the Hosted Services must have multi-factor authentication for privileged/administrative access.

4. Unauthorized Access. Contractor may not access, and shall not permit any access to, State Systems, in whole or in part, whether through Contractor’s Systems or otherwise, without the State’s express prior written authorization. Such authorization may be revoked by the State in writing at any time in its sole discretion. Any access to State Systems must be solely in accordance with the Contract and this Schedule, and in no case exceed the scope of the State’s authorization pursuant to this **Section 4**. All State-authorized connectivity or attempted connectivity to State Systems shall be only through the State’s security gateways and firewalls and in compliance with the State’s security policies set forth in the Contract as the same may be supplemented or amended by the State and provided to Contractor from time to time.

5. Contractor Systems. Contractor will be solely responsible for the information technology infrastructure, including all computers, software, databases, electronic systems (including database management systems) and networks used by or for Contractor in connection with the Services (“**Contractor Systems**”) and shall prevent unauthorized access to State Systems through the Contractor Systems.

6. Security Audits. During the Term, Contractor will:

6.1 maintain complete and accurate records relating to its data protection practices, IT security controls, and the security logs of any of the State’s Confidential Information, including any backup, disaster recovery or other policies, practices or procedures relating to the State’s Confidential Information and any other information relevant to its compliance with this Schedule;

6.2 upon the State’s request, make all such records, appropriate personnel and relevant materials available during normal business hours for inspection and audit by the State or an independent data security expert that is reasonably acceptable to Contractor, provided that the State: (i) gives Contractor at least five (5) Business Days prior notice of any such audit; (ii) undertakes such audit no more than once per calendar year, except for good cause shown; and (iii) conducts or causes to be conducted such audit

in a manner designed to minimize disruption of Contractor's normal business operations and that complies with the terms and conditions of all data confidentiality, ownership, privacy, security and restricted use provisions of the Contract. The State may, but is not obligated to, perform such security audits, which shall, at the State's option and request, include penetration and security tests, of any and all Contractor Systems and their housing facilities and operating environments; and

6.3 if requested by the State, provide a copy of Contractor's FedRAMP System Security Plan. The System Security Plan will be recognized as Contractor's Confidential Information.

7. **Nonexclusive Remedy for Security Breach**. Any failure of the Services to meet the requirements of this Schedule with respect to the security of any State Data or other Confidential Information of the State, including any related backup, disaster recovery or other policies, practices or procedures, is a material breach of the Contract for which the State, at its option, may terminate the Contract immediately upon written notice to Contractor without any notice or cure period, and Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination.