



**STATE OF MICHIGAN PROCUREMENT**  
Department Technology, Management and Budget

**NOTICE OF CONTRACT**

NOTICE OF CONTRACT NO. **250000000015**

between

THE STATE OF MICHIGAN

and

<b>CONTRACTOR</b>	Tyler Technologies, Inc.	<b>STATE</b>	Program Manager	Multiple	Multiple
	840 West Long Lake Road				
	Troy Michigan 48098				
	Elizabeth Des Meules		Contract Administrator	Kristine Mills	DTMB
	248-269-1000 ext. 1985			517-242-6402	
	Elizabeth.DesMeules@tylertech.com			millsk11@michigan.gov	
	CV0136837				

CONTRACT SUMMARY			
DESCRIPTION: Computer Aided Dispatch (CAD) System for Michigan State Police (MSP).			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
11/1/2024	10/31/2029	5 - 1 Year	10/31/2029
PAYMENT TERMS		DELIVERY TIMEFRAME	
Net 45		N/A	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-card <input type="checkbox"/> Payment Request (PRC) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS			
N/A			
MISCELLANEOUS INFORMATION			
THIS IS NOT AN ORDER. This Contract Agreement is awarded on the basis of the State's inquiry bearing the solicitation number 230000002656. Orders for Delivery will be issued directly by the Department through the issuance of a Delivery Order (DO).			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION			<b><u>\$6,005,950.00</u></b>

**Program Managers  
for  
Multi-Agency and Statewide Contracts**

AGENCY	NAME	PHONE	EMAIL
DTMB	Jim Coggin	517-243-5265	CogginJ@michigan.gov
MSP	Jonathon Whitford	517-512-4068	WhitfordJ@michigan.gov

**FOR THE CONTRACTOR:**

---

**Company Name**

---

**Authorized Agent Signature**

---

**Authorized Agent (Print or Type)**

---

**Date**

**FOR THE STATE:**

---

**Signature**

---

**Name and Title**

---

**Agency**

---

**Date**

# SOFTWARE CONTRACT TERMS AND CONDITIONS

---

These Terms and Conditions, together with all Schedules (including the Statement(s) of Work), Exhibits and any other applicable attachments or addenda (Collectively this “Contract”) are agreed to between the State of Michigan (the “**State**”) and Tyler Technologies, Inc. (“**Contractor**”), a Delaware CORPORATION. This Contract is effective on November 1, 2024 (“**Effective Date**”), and unless terminated, will expire on October 31, 2029 (the “**Term**”).

This Contract may be renewed for up to 5 additional 1-year periods. Renewal is at the mutual agreement the State and Contractor and will automatically extend the Term of this Contract. The State and Contractor will document their exercise of renewal options via a Change Notice signed by both parties.

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

“**Acceptance**” has the meaning set forth in **Section 9**.

“**Acceptance Tests**” means such tests as may be conducted in as described in **Section 9** and any applicable Statement of Work to determine whether the Software meets the 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 18**.

“**Approved Third Party Components**” means all third party components, including Open-Source Components, that are included in or used in connection with the Software and are specifically identified by Contractor in the Contractor’s Bid Response or as part of the State’s Security Accreditation Process defined in Schedule E – Data Security Requirements.

“**Authorized Users**” means all Persons authorized by the State to access and use the Software under this Contract, subject to the maximum number of users specified in the applicable Statement of Work.

**“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 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 a Statement of Work.

**“Contract Change”** has the meaning set forth in **Subsection 2.2**.

**“Change Notice”** means a writing executed by the parties to the Contract memorializing a change to the Contract.

**“Change Proposal”** has the meaning set forth in **Subsection 2.2**.

**“Change Request”** has the meaning set forth in **Subsection 2.2**.

**“Confidential Information”** has the meaning set forth in **Subsection 22.1**.

**“Configuration”** means State-specific changes made 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 Schedule A or subsequent Change Notices.

**“Contractor”** has the meaning set forth in the preamble.

**“Contractor’s Bid Response”** means the Contractor’s proposal submitted in response to the Request for Proposal.

**“Contractor Hosted”** means the Hosted Services are provided by Contractor or one or more of its Permitted Subcontractors.

**“Contractor Personnel”** means all employees of Contractor or any subcontractors or Permitted Subcontractors involved in the performance of Services hereunder.

**“Contractor Project Manager”** means the individual appointed by Contractor and identified in Schedule A or subsequent Change Notices to serve as the primary contact with regard to services, to monitor and coordinate the day-to-day activities of this

Contract, and to perform other duties as may be further defined in this Contract, including an applicable Statement of Work.

**“Customization”** means State-specific changes to the Software's underlying Source Code or structural data model changes.

**“Defect”** means a failure of the Software to conform to the functional descriptions set forth in the Contract.

**“Deliverables”** means the Software, Services, Documentation, any Hardware, 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 a Statement of Work and all Work Product.

**“Digital Accessibility Standards”** means the accessibility standards provided in the SOM Digital Standards, located at <https://www.michigan.gov/standards>.

**“Disaster Recovery Plan”** refers to the set(s) of documents, instructions, and procedures which enable the Contractor to respond to accidents, disasters, emergencies, or threats without any stoppage or hindrance in its key operations and to the actions the Contractor takes to meet the Recovery Point and Recovery Time Objectives.

**“Documentation”** means all 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 Deliverable.

**“DTMB”** means the Michigan Department of Technology, Management and Budget.

**“Effective Date”** has the meaning set forth in the preamble.

**“Fees”** means the fees set forth in the Pricing Schedule attached as **Schedule B**.

**“Financial Audit Period”** has the meaning set forth in **Subsection 23.1**.

**“Hardware”** means all computer hardware or other equipment provided by Contractor under this Contract, if any, including but not limited to any related accessories.

**“Harmful Code”** means any software, hardware or other technologies, devices or means, the purpose or effect of which is to: (a) permit unauthorized access to, or to destroy, disrupt, disable, encrypt, modify, copy, or otherwise harm or impede in any manner, any (i) computer, software, firmware, data, hardware, system or network, or (ii) any application or function of any of the foregoing or the integrity, use or operation of any data Processed thereby; or (b) prevent the State or any Authorized User from accessing or using the Services as intended by this Contract, and includes any virus, bug, trojan horse, worm, backdoor or other malicious computer code and any time bomb or drop dead device.

**“Hosted Services”** means software-as-a-service consisting of hosting, support, management and operation of the Operating Environment and Software, including providing access and use to the Software by the State and its Authorized Users, and also including any services and facilities related to disaster recovery obligations. Hosted Services do not include support of the State’s on-premise infrastructure operating systems, or training, consulting or other professional services.

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

**“Integration Testing”** has the meaning set forth in **Section 9**.

**“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 Contract.

**“Loss or Losses”** means all losses, including but not limited to, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees and the 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 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 a 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 a Statement of Work.

**“New Version”** means any new version of the Software, including any updated Documentation, 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 failure or failures of a Deliverable, to conform to the requirements of this Contract.

**“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.

**“Operating Environment”** means, collectively, the platform, environment and conditions on, in or under which the Software is intended to be installed and operate, as set forth in a Statement of Work, including such structural, functional and other features, conditions and components as hardware, operating software, system architecture, configuration, computing hardware, ancillary equipment, networking, software, firmware, databases, data, and electronic systems (including database management systems).

**“PAT”** means a document or product accessibility template, including any Information Technology Industry Council Voluntary Product Accessibility Template or



VPAT®, that specifies how information and software products, such as websites, applications, software and associated content, conform to the Digital Accessibility Standards.

**“Permitted Subcontractor”** means any third party hired by Contractor to perform Services for the State under this Contract, have access to or have the ability to control access to State Data.

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

**“Pricing Schedule”** means the schedule attached as **Schedule B**.

**“Process”** means to perform any operation or set of operations on any data, information, material, work, expression or other content, including to (a) collect, receive, input, upload, download, record, reproduce, store, organize, combine, log, catalog, cross-reference, manage, maintain, copy, adapt, alter, translate or make other improvements or derivative works, (b) process, retrieve, output, consult, use, disseminate, transmit, submit, post, transfer, disclose or otherwise provide or make available, or (c) block, erase or destroy. **“Processing”** and **“Processed”** have correlative meanings.

**“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.

**“Services”** means any of the services, including but not limited to, Hosted Services, Contractor is required to or otherwise does provide under this Contract.

**“Service Level Agreement”** means the schedule attached as **Schedule D**, setting forth the Support Services Contractor will provide to the State, and the parties' additional rights and obligations with respect thereto.

**“Support Call Process”** means the support call process attached as Exhibit 1 to Schedule D.

**“Site”** means any physical location(s) designated by the State in, or in accordance with, this Contract or a Statement of Work for delivery and installation of the Deliverable, if applicable.

**“Software”** means Contractor’s software as set forth in this Contract, and any Maintenance Releases or New Versions provided to the State and any Customization or Configurations, including any integrations, custom modifications, and/or other related interfaces and provided to the State pursuant to this Contract, and all copies of the foregoing permitted under this Contract. The Software also includes Approved Third Party Components.

**“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 understand, build, operate, support, maintain and develop modifications, upgrades, updates, adaptations, enhancements, new versions and other derivative works and improvements of, and to develop computer programs compatible with, the Software.

**“Specifications”** means, for the Software, the specifications collectively set forth in the Business Requirements Specification, Technical Specification, Documentation, Request for Proposal or Contractor’s Bid Response, if any, for such Software, or elsewhere in a Statement of Work.

**“State”** means the State of Michigan.

**“State Data”** has the meaning set forth in **Section 21**.

**“State Hosted”** means the Hosted Services are not provided by Contractor or one or more of its Permitted Subcontractors.

**“State Materials”** means all materials and information, including but not limited to documents, data, know-how, ideas, methodologies, specifications, software, hardware, 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 Program Managers”** are the individuals appointed by the State, or their designees, to (a) monitor and coordinate the day-to-day activities of this Contract; (b) co-sign off on Acceptance of the Deliverables; and (c) perform other duties as may be

specified in a Statement of Work. Program Managers will be identified in Schedule A or subsequent Change Notices.

**“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.

**“Statement of Work”** means any statement of work entered into by the parties and incorporated into this Contract. The initial Statement of Work is attached as **Schedule A**.

**“Stop Work Order”** has the meaning set forth in **Section 15**.

**“Support Services”** means the maintenance and support services Contractor is required to or otherwise does provide to the State under the Support Call Process and Service Level Agreement.

**“System”** has the meaning set forth in **Schedule I**.

**“System Acceptance”** has the meaning set forth in **Schedule I**.

**“System Integration Testing”** has the meaning set forth in **Schedule I**.

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

**“Term”** has the meaning set forth in the preamble.

**“Testing Period”** has the meaning set forth in **Section 9**.

**“Transition Period”** has the meaning set forth in **Section 16**.

**“Transition Responsibilities”** has the meaning set forth in **Section 16**.

**“Unauthorized Removal”** has the meaning set forth in **Subsection 2.5**.

**“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 or on behalf of the State, including any and all works, inventions, data, analyses and other information and materials resulting from any use of

the Software by or on behalf of the State under this Contract, except that User Data does not include the Software 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 without the inclusion of user derived Information or additional user input.

**“Work Product”** means all State-specific deliverables, if any, that Contractor is required to, or otherwise does, provide to the State under this Contract including but not limited to Customizations, application programming interfaces, 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.

**2. Duties of Contractor.** Contractor will provide Deliverables pursuant to Statement(s) of Work entered into under this Contract. Contractor will provide all Deliverables in a timely, professional manner and in accordance with the terms, conditions, and Specifications set forth in this Contract and the Statement(s) of Work.

**2.1 Statement of Work Requirements.** No Statement of Work will be effective unless signed by each party’s Contract Administrator. The term of each Statement of Work will commence on the parties’ full execution of a Statement of Work and terminate when the parties have fully performed their obligations. The terms and conditions of this Contract will apply at all times to any Statements of Work entered into by the parties and incorporated into this Contract. The State will have the right to terminate such Statement of Work as set forth in **Section 16**.

**2.2 Change Control Process.** The State may at any time request in writing (each, a **“Change Request”**) changes to the Contract generally or any Statement of Work, including changes to the Services and Implementation Plan (each, a **“Contract Change”**). Upon the State’s submission of a Change Request, the parties will evaluate and implement all Changes in accordance with this Section.

(a) As soon as reasonably practicable, and in any case within 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 Deliverables;

(ii) an amended Implementation Plan reflecting: (A) the schedule for commencing and completing any additional or modified Deliverables; and (B) the effect of such Changes, if any, on completing any other Services under a 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 only the increase or decrease in time and expenses Contractor requires to carry out the Change.

(b) Within 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, each parties' Contractor Administrator will sign a Change Notice.

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

(i) require Contractor to perform or provide the Deliverables under the existing Statement of Work without the Change;

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

(iii) initiate a Dispute Resolution Procedure.

(d) No Change will be effective until the parties have executed a Change Notice. Notwithstanding the foregoing, no Statement of Work or Change Notice executed after the Effective Date will construed to amend or modify this Contract in any way, unless it specifically states its intent to do so and cites the section or sections amended. Except as the State may request in its Change Request or otherwise in writing, Contractor must continue to perform its obligations in accordance with a Statement of Work pending negotiation and

execution of a Change Notice. Contractor will use its best 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 Nonconformities 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.

### 2.3 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) require such Contractor Personnel to agree in writing to the confidentiality provisions contained in this Contract; and

(iii) upon request, or as otherwise specified in a Statement of Work, perform background checks on all Contractor Personnel 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. Pursuant to Michigan law, all agencies subject to IRS Pub. 1075 are required to ask the Michigan State Police to perform fingerprint background checks on all employees, including Contractor and subcontractor employees, who may have access to any database of information maintained by the federal government that contains confidential or personal information, including, but not limited to, federal tax information. Further, pursuant to Michigan law, any agency described above is prohibited from providing Contractors or subcontractors with the result of such background check. For more information, please see Michigan Public Act 427 of 2018.

(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.

2.4 Contractor Project Manager. Throughout the Term of this Contract, Contractor must maintain a Contractor employee acceptable to the State to serve as Contractor Project Manager, who will be considered Key Personnel of Contractor.

(a) Contractor 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 Project Manager must attend all regularly scheduled meetings as set forth in the Implementation Plan and will otherwise be available as set forth in a Statement of Work.

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

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

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

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

(iv) Contractor Project Manager assumes a different role within Contractor's corporation that is not a project manager role.

(d) Upon the occurrence of any event set forth in **Subsections 2.4(c)(i-iii)** above, Contractor will promptly replace its Contractor Project Manager. Such replacement will be subject to the State's prior written approval, which will not be unreasonably withheld.

## 2.5 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 Program Managers or their designees, 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, which will not be



unreasonably withheld. 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, an assumption of a new role within Contractor's corporation or for cause termination of the Key Personnel's employment. Any Unauthorized Removal may be considered by the State to be a material breach of this Contract.

**2.6 Subcontractors.** Contractor must obtain prior written approval of the State, which consent may be given or withheld in the State's sole discretion, before engaging any Permitted Subcontractor to provide Services to the State under this Contract. Third parties otherwise retained by Contractor to provide Contractor or other clients of contractor with services are not Permitted Subcontractors, and therefore do not require prior approval by the State. Engagement of any subcontractor or Permitted Subcontractor by Contractor does not relieve Contractor of its representations, warranties or obligations under this Contract. Without limiting the foregoing, Contractor will:

- (a) be responsible and liable for the acts and omissions of each such subcontractor (including such Permitted Subcontractor and Permitted Subcontractor's employees who, to the extent providing Deliverables, will be deemed Contractor Personnel) to the same extent as if such acts or omissions were by Contractor or its employees;
- (b) name the State a third-party beneficiary under Contractor's Contract with each Permitted Subcontractor with respect to the Services;
- (c) 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
- (d) notify the State of the location of the Permitted Subcontractor and indicate if it is located within the continental United States.

**3. Notices.** All notices and other communications required or permitted under this Contract must be in writing and will be considered given and received: (a) when verified by written receipt if sent by courier; (b) when actually received if sent by mail without verification of receipt; or (c) when verified by automated receipt or electronic logs if sent by facsimile or email.

If to State:	If to Contractor:
Kristine Mills 320 S. Walnut St. 2nd Floor Lansing, MI 48909-7526 millsk11@michigan.gov 517-242-6402	Abigail Diaz Tyler Technologies, Inc. Attn: Chief Legal Officer 1 Tyler Drive Yarmouth, ME 04096 abigail.diaz@tylertech.com (800) 772-2260

**4. Insurance.** Contractor must maintain the minimum insurances identified in the Insurance Schedule attached as **Schedule C**.

## **5. Software License.**

### **5.1 RESERVED.**

**5.2 Subscription License.** If the Software is Contractor Hosted and Contractor is providing the State access to use its Software during the Term of the Contract only, then:

(a) Contractor hereby grants to the State, exercisable by and through its Authorized Users, a nonexclusive, irrevocable right-during the Term and such additional periods, if any, as Contractor is required to perform Services under this Contract or any Statement of Work, to:

(i) access and use the Software, including in operation with other software, hardware, systems, networks and services, for the State's governmental purposes, including for Processing State Data;

(ii) generate, print, copy, upload, download, store and otherwise Process all GUI, audio, visual, digital and other output, displays and other content as may result from any access to or use of the Software;

(iii) prepare, reproduce, print, download and use a reasonable number of copies of the Specifications and Documentation for any use of the Software under this Contract; and

(iv) access and use the Software for all required governmental purposes, including such non-production uses and applications as may be necessary or useful for the effective use of the Software hereunder, including for purposes of analysis, configuration, integration, testing, training, maintenance which access and use will be without charge and not included for any purpose in any calculation of the State's or its Authorized Users' use of the Software, including for purposes of assessing any Fees or other consideration payable to Contractor or determining any excess use of the Software as described in **Subsection 5.2(c)** below.

(b) License Restrictions. The State will not: (a) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer or otherwise make the Software available to any third party, except as expressly permitted by this Contract or in any Statement of Work; or (b) use or authorize the use of the Software or Documentation in any manner or for any purpose that is unlawful under applicable Law.

(c) Use. The State will pay Contractor the corresponding Fees set forth in a Statement of Work or Pricing Schedule for all Authorized Users access and use of the Software.

**5.3 Certification.** To the extent that a License granted to the State is not unlimited, Contractor may request written certification from the State regarding use of the Software for the sole purpose of verifying compliance with this **Section**. Such written certification may occur no more than once in any 24 month period during the Term of the Contract. The State will respond to any such request within 45 calendar days of receipt. If the State's use is greater than contracted, Contractor may invoice the State for any unlicensed use (and related support) pursuant to the terms of this Contract at the rates set forth in **Schedule B**, and the unpaid license and support fees shall be payable in accordance with the terms of the Contract. Payment under this provision shall be Contractor's sole and exclusive remedy to cure these issues.

**5.4 State License Grant to Contractor.** The State hereby grants to Contractor a limited, non-exclusive, non-transferable license (i) to use the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos, solely in accordance with the State's specifications, and (ii) to display, reproduce, distribute and transmit in digital form the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos in connection with promotion of the Services as communicated to Contractor by the State. Use of the State's (or individual agency's, department's or division's) name, trademarks,

service marks or logos will be specified in the applicable Statement of Work. Contractor is provided a limited license to State Materials for the sole and exclusive purpose of providing the Services.

**6. Third Party Components.** At least 30 days prior to adding new Third Party Components, Contractor will provide the State with notification information identifying and describing the addition. Throughout the Term, on an annual basis, Contractor will provide updated information identifying and describing any Approved Third Party Components included in the Software.

## **7. Intellectual Property Rights**

### **7.1 Ownership Rights in Software**

(a) For purposes of this **Section 7** only, the term “Software” does not include Customizations.

(b) Subject to the rights and licenses granted by Contractor in this Contract and the provisions of **Subsection 7.1(c)**:

(i) Contractor reserves and retains its entire right, title and interest in and to all Intellectual Property Rights arising out of or relating to the Software; and

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

(c) 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 Materials, User Data, including all Intellectual Property Rights arising therefrom or relating thereto.

**7.2** The State is and will be the sole and exclusive owner of all right, title, and interest in and to all Work Product developed exclusively for the State under this Contract, including all Intellectual Property Rights. In furtherance of the foregoing:

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

(b) to the extent any Work Product, 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 Work Product, including all Intellectual Property Rights; 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 Work Product.

## **8. Software Implementation.**

8.1 Implementation. Contractor will, as applicable; 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 criteria set forth in a Statement of Work and the Implementation Plan.

8.2 Site Preparation. Unless otherwise set forth in a Statement of Work, Contractor is responsible for ensuring the relevant Operating Environment is set up and in working order to allow Contractor to install and configure the Software and provide the State with access on or prior to the applicable Milestone Date. Contractor will provide the State with such notice as is specified in a Statement of Work, prior to installing and providing access to the Software to give the State sufficient time to prepare for Contractor’s installation of the Software.

## **9. Software Acceptance Testing.**

### **9.1 Acceptance Testing.**

(a) Unless otherwise specified in a Statement of Work, upon installation of the Software, or in the case of Contractor Hosted Software, when Contractor notifies the State in writing that the Hosted Services are ready for use in a production environment, Acceptance Tests will be conducted as set forth in this **Section 9** to ensure the Software conforms to the requirements of this Contract, including the applicable Specifications and Documentation.

(b) All Acceptance Tests will take place at the designated Site(s) in the Operating Environment described in a Statement of Work, commence on the Business Day following installation of the Software, or the receipt by the State of the notification referenced in **Subsection 9.1(a)**, and be conducted diligently for up to 30 Business Days, or such other period as may be set forth in a Statement of Work (the “**Testing Period**”). Acceptance Tests will be conducted

by the party responsible as set forth in a Statement of Work or, if a 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.

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

(a) Upon delivery and installation of any application programming interfaces, Configuration or Customizations, or any other applicable Work Product, to the Software under a Statement of Work, additional Acceptance Tests will be performed on the modified 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 this **Section**.

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

9.3 Notices of Completion, Non-Conformities, and Acceptance. Within 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 Nonconformity in the tested Software.

(a) If such notice is provided by either party and identifies any Nonconformities, the parties' rights, remedies, and obligations will be as set forth in **Subsection 9.4** and **Subsection 9.5**.

(b) If such notice is provided by the State, is signed by the State Program Managers or their designees, and identifies no Nonconformities, 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 30 Business Days to use the Software in the Operating Environment and determine, in the exercise of its sole discretion, whether it is satisfied that the Software contains no Nonconformities, on the completion of which the State will, as appropriate:

(i) notify Contractor in writing of Nonconformities 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 **Subsection 9.4** and **Subsection 9.5**; or

(ii) provide Contractor with a written notice of its Acceptance of such Software, which must be signed by the State Program Managers or their designees.

**9.4 Failure of Acceptance Tests.** If Acceptance Tests identify any Non-Conformities, Contractor, at Contractor's sole cost and expense, will remedy all such Nonconformities and re-deliver the Software, in accordance with the requirements set forth in the Contract. Redelivery will occur as promptly as commercially possible and, in any case, within 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 **Subsection 9. (a)** or **(c)(i)**, identifying any Nonconformities.

**9.5 Repeated Failure of Acceptance Tests.** If Acceptance Tests identify any Nonconformity 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 9**;

(b) deem the failure to be a material breach of this Contract and a Statement of Work and terminate this Contract in accordance with **Section 16**.

9.6 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 **Subsection 9.3(b)**, or **(c)(ii)**. Acceptance of the Software may be conditioned upon System Acceptance, if Contractor is providing Hardware, under the terms of this Contract.

**10. Reserved.**

**11. Assignment.** Contractor may not assign this Contract or any of its rights or delegate any of its duties or obligations hereunder, voluntarily, or involuntarily, whether by merger (regardless of whether it is the surviving or disappearing entity), conversion, consolidation, dissolution, or operation of law to any other party without the prior written approval of the State. Upon notice to Contractor, the State, in its sole discretion, may assign in whole or in part, its rights or responsibilities under this Contract to any other governmental entity if such assignment is made reasonably necessary by operation of controlling law or regulation. If the State determines that a novation of the Contract to a third party is necessary, Contractor will agree to the novation and provide all necessary documentation and signatures.

**12. Change of Control.** Contractor will notify the State, within 30 days of any public announcement or otherwise once legally permitted to do so, of a change in Contractor’s organizational structure or ownership. For purposes of this Contract, a change in control means any of the following:

- (a) a sale of more than 50% of Contractor’s stock;
- (b) a sale of substantially all of Contractor’s assets;
- (c) a change in a majority of Contractor’s board members;
- (d) consummation of a merger or consolidation of Contractor with any other entity;
- (e) a change in ownership through a transaction or series of transactions;
- (f) or the board (or the stockholders) approves a plan of complete liquidation.

A change of control does not include any consolidation or merger effected exclusively to change the domicile of Contractor, or any transaction or series of transactions principally for bona fide equity financing purposes. In the event of a change of control,



Contractor must require the successor to assume this Contract and all of its obligations under this Contract.

### **13. Invoices and Payment.**

13.1 Invoices must conform to the requirements communicated from time-to-time by the State. All undisputed amounts are payable within 45 days of the State's receipt. Contractor may only charge for Deliverables provided as specified in Statement(s) of Work. Invoices must include an itemized statement of all charges.

13.2 The State has the right to withhold payment of any disputed amounts until the parties agree as to the validity of the disputed amount. The State will notify Contractor of any dispute within a reasonable time. Payment by the State will not constitute a waiver of any rights as to Contractor's continuing obligations, including claims for deficiencies or substandard Deliverables. Contractor's acceptance of final payment by the State constitutes a waiver of all claims by Contractor against the State for payment under this Contract, other than those claims previously filed in writing on a timely basis and still disputed.

13.3 The State will only disburse payments under this Contract through Electronic Funds Transfer (EFT). Contractor must register with the State at <http://www.michigan.gov/SIGMAVSS> to receive electronic fund transfer payments. If Contractor does not register, the State is not liable for failure to provide payment.

13.4 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 then due and owing to it by Contractor against any amount payable by the State to Contractor under this Contract.

13.5 Taxes. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Deliverables purchased under this Contract are for the State's exclusive use. Notwithstanding the foregoing, all Fees are exclusive of taxes, and Contractor is responsible for all sales, use and excise taxes, and any other similar taxes, duties and charges of any kind imposed by any federal, state, or local governmental entity on any amounts payable by the State under this Contract.

13.6 Pricing/Fee Changes. All Pricing set forth in this Contract will not be increased, except as otherwise expressly provided in this Section.

(a) The Fees 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.

#### **14. Liquidated Damages**

14.1 The parties understand and agree that any liquidated damages (which includes but is not limited to applicable credits) set forth in this Contract are reasonable estimates of the State's damages in accordance with applicable law.

14.2 The parties acknowledge and agree that Contractor could incur liquidated damages for more than one event.

14.3 The assessment of liquidated damages will not constitute a waiver or release of any other remedy the State may have under this Contract for Contractor's breach of this Contract, including without limitation, the State's right to terminate this Contract for cause and the State will be entitled in its discretion to recover actual damages caused by Contractor's failure to perform its obligations under this Contract. However, the State will reduce such actual damages by the amounts of liquidated damages received for the same events causing the actual damages.

14.4 Amounts due the State as liquidated damages may be set off against any Fees payable to Contractor under this Contract, or the State may bill Contractor as a separate item and Contractor will promptly make payments on such bills.

**15. Stop Work Order.** The State may suspend any or all activities under the Contract at any time. The State will provide Contractor a written stop work order detailing the suspension. Contractor must comply with the stop work order upon receipt. Within 90 calendar 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 the Contract or delivery order pursuant to Section 16. The State will not pay for activities that have been suspended, Contractor's lost profits, or any additional compensation during a stop work period.

**16. Termination, Expiration, Transition.** The State may terminate this Contract or any portion thereof, in accordance with the following provisions.

16.1 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, as determined by the State:

- 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. 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 the State terminates this Contract under this Subsection 16.1, the State will issue a termination notice specifying whether Contractor must:

- (i) cease performance immediately in the event of a breach of (a)(i) or (a)(ii) above, or as otherwise provided elsewhere in this Contract, or
- (ii) continue to perform as specified for all other breaches that the State deems curable and which the State will provide a 30-day right to cure.
- (iii) 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 Subsection 16.2.

(c) Contractor must submit all invoices for Services accepted by the State and/or Services not disputed by the State within 30 days of the date of termination. Failure to submit an invoice within that timeframe will constitute a waiver by Contractor for any amounts due to Contractor for Services accepted by the State under this Contract. The State will only pay for amounts due to Contractor for Services accepted by the State and/or Services delivered and not disputed 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 any applicable credits owed to the State under this Contract. Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination.

16.2 Termination for Lack of Appropriations and Convenience. The State may immediately terminate this Contract in whole or in part, in the event of appropriation

or budget shortfalls without notice. In all other instances, following the third anniversary of the Effective Date, the State may terminate this Contract in whole or in part, without penalty and for any reason or no reason, by providing sixty (60) days written notice. The termination notice will specify whether Contractor must:

(a) cease performance immediately. Contractor must submit all invoices for Services accepted by the State and for Services delivered and not disputed by the State within 30 days of the date of termination. Failure to submit an invoice within that timeframe will constitute a waiver by Contractor for any amounts due to Contractor for such Services.

(b) continue to perform in accordance with Subsection 16.3. If the State terminates this Contract for convenience, the State will pay all reasonable costs, as determined by the State, for State approved Transition Responsibilities to the extent the funds are available.

#### 16.3 Transition Responsibilities.

(a) 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 State’s Data to the State or its designees. Such transition assistance may include but is not limited to:

(i) continuing to perform the Services at the established Contract rates;

(ii) taking all reasonable and necessary measures to transfer the State’s Data to the State or the State’s designee. Contractor will provide the State or the State’s designee the State’s Data in a mutually agreed upon file format within 30 calendar days following the termination or expiration of the Contract.

(iii) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, and comply with **Section 22**, including without limitation, the return or destruction of State Data at the conclusion of the Transition Period; and

(iv) 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.

## **17. Indemnification.**

17.1 General and Intellectual Property 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 those required to establish the right to indemnification), arising out of or relating to:

- (a) any infringement, misappropriation, or other violation of any type of Intellectual Property Right of any third party;
- (b) 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);
- (c) any violation of a law by Contractor (or any of Contractor’s employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable) applicable to Contractor; and
- (d) any third-party claim arising under Section 21.5 as a result of an action or inaction by Contractor.

17.2 Indemnification Procedure. The State will notify Contractor in writing if 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 satisfaction of the State, demonstrate its financial ability to carry out these obligations. The State is entitled to:

- (a) regular updates on proceeding status;
- (b) participate in the defense of the proceeding at its own cost;
- (c) employ its own counsel at its own cost; and to
- (d) retain control of the defense, at its own cost and expense, if the State deems necessary in accordance with law applicable to the State. 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. Any litigation activity on behalf of the State or any of its subdivisions 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.

17.3 The State is constitutionally prohibited from indemnifying Contractor or any third parties.

## **18. Infringement Remedies.**

18.1 For purposes of this Section 18, the definition of Deliverables does not include Services. The remedies set forth in this Section 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.

18.2 If any Deliverable, or any component thereof, other than State Materials, is found to be infringing or if any use of any Deliverable, 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:

- (a) procure for the State the right to continue to use such Deliverable, or component thereof, to the full extent contemplated by this Contract; or
- (b) modify or replace the materials that infringe or are alleged to infringe ("**Allegedly Infringing Materials**") to make the Deliverable and all of its components non-infringing while providing fully equivalent features and functionality.

18.3 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:

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

18.4 If Contractor directs the State to cease using any Deliverable under Subsection 18.3, the State, at its sole discretion, will be entitled to declare such a direction from the Contractor to cease use a material breach of the Contract and may terminate this Contract under Section 16. Unless the claim arose against the

Deliverable independently of any of the actions specified below, Contractor will have no liability for any claim of infringement arising solely from:

- (a) Contractor's compliance with any designs, specifications, or instructions of the State; or
- (b) modification of the Deliverable by the State without the prior knowledge and approval of Contractor.

## **19. Disclaimer of Damages and Limitation of Liability.**

19.1 The Parties' Disclaimer of Damages. NEITHER THE STATE NOR CONTRACTOR WILL BE LIABLE, 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.

19.2 The Parties' Limitation of Liability. IN NO EVENT WILL EITHER THE STATE'S OR CONTRACTOR'S AGGREGATE LIABILITY TO ONE ANOTHER 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 THREE TIMES THE ANNUAL SAAS FEES PAYABLE UNDER THIS CONTRACT AT THE RATE PAYABLE DURING THE ANNUAL TERM IN WHICH THE CLAIM AROSE. HOWEVER, NOTWITHSTANDING THE FOREGOING, CONTRACTOR'S LIABILITY TO STATE FOR ANY CLAIMS OR LIABILITIES BASED ON CONTRACTOR'S BREACH OF SECTION 21.5, LOSS OR COMPROMISE OF STATE DATA, WILL NOT EXCEED SIX TIMES THE ANNUAL SAAS FEES PAYABLE UNDER THIS CONTRACT AT THE RATE PAYABLE DURING THE ANNUAL TERM IN WHICH THE CLAIM AROSE.

19.3 **Exceptions.** Subsections (a) (Disclaimer of Damages) and (b) (Limitation of Liability) above, will not apply to: (i) Contractor's obligation to indemnify under this Contract; (ii) damages arising from either party's bad faith or intentional misconduct; and (iii) amounts due or obligations under this Contract (regardless of how named) providing for liquidated damages.

**20. Disclosure of Litigation, or Other Proceeding.** Contractor must notify the State within 14 calendar days of receiving notice of any litigation, investigation, arbitration, or other proceeding (collectively, “**Proceeding**”) involving Contractor, a Permitted Subcontractor, or an officer or director of Contractor or Permitted Subcontractor, that arises during the term of the Contract, including:

- (a) a criminal Proceeding;
- (b) a parole or probation Proceeding;
- (c) a Proceeding under the Sarbanes-Oxley Act;
- (d) a civil Proceeding involving:
  - (i) a claim that might reasonably be expected to adversely affect Contractor’s viability or financial stability; or
  - (ii) a governmental or public entity’s claim or written allegation of fraud ; or(e) a Proceeding involving any license that Contractor is required to possess in order to perform under this Contract.

**21. State Data.**

21.1 Ownership. The State’s data (“**State Data**”), which will be treated by Contractor as Confidential Information, includes:

- (a) User Data; and
- (b) any other data collected, used, Processed, stored, or generated 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) protected 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.

21.2 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.

21.3 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, any applicable Statement of Work, and applicable law;
- (c) keep and maintain State Data in the continental United States and
- (d) not use, sell, rent, transfer, mine, distribute, commercially exploit, 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. Contractor’s misuse of State Data may violate state or federal laws, including but not limited to MCL 752.795.

21.4 Third-Party Requests. Contractor will immediately notify the State upon receipt of any third-party requests which in any way might reasonably require access to State Data. Contractor will notify the State Program Managers or their designees by the fastest means available and also in writing. Contractor must provide such notification within twenty-four (24) hours from Contractor’s receipt of the request. Contractor will not respond to subpoenas, service of process, FOIA requests, and other legal requests related to the State without first notifying the State. Upon request by the State, Contractor must provide to the State, its proposed response to the third-party request with adequate time for the State to review, and, as it deems necessary, to revise the response, object, or take other action.

21.5 Loss or Compromise of Data. In the event of a data breach, as such term is defined by applicable law, or any act, error or omission, negligence, misconduct, or breach on the part of Contractor that compromises or is reasonably suspected to compromise the security, confidentiality, integrity, or availability 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 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 reasonably 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 30 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 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 incurred by Contractor associated with the occurrence,
- (g) be responsible for restoring lost State Data in the manner and on the schedule set by the Service Level Agreement; and
- (h) provide to the State a detailed plan within 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.

21.6 The parties agree that any damages arising out of a breach of the terms set forth in this Section are to be considered direct damages and not consequential damages.

**22. Non-Disclosure of Confidential Information.** The parties acknowledge that each party may be exposed to or acquire communication or data of the other party that is confidential, privileged communication not intended to be disclosed to third parties.

22.1 Meaning of Confidential Information. For the purposes of this Contract, 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; and, (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: (a) 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). For purposes of this Contract, in all cases and for all matters, State Data is deemed to be Confidential Information.

**22.2 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 and Permitted Subcontractor's Representatives may be required to execute a separate agreement to be bound by the provisions of this **Subsection 22.2**.

**22.3 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.

**22.4 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.

22.5 Surrender of Confidential Information. Upon termination or expiration of this Contract or a Statement of Work, in whole or in part, each party must, within 30 calendar days from the date of termination or expiration, 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. Upon confirmation from the State, of receipt of all data, Contractor must permanently sanitize or destroy the State's Confidential Information, including State Data, from all media including backups using National Security Agency ("NSA") and/or National Institute of Standards and Technology ("NIST") (NIST Guide for Media Sanitization 800-88) data sanitization methods or as otherwise instructed by the State. If the State determines that the return of any Confidential Information is not feasible or necessary, Contractor must destroy the Confidential Information as specified above. The Contractor must certify the destruction of Confidential Information (including State Data) in writing within 5 Business Days from the date of confirmation from the State.

## **23. Records Maintenance, Inspection, Examination, and Audit.**

23.1 Right of Audit. Pursuant to MCL 18.1470, 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 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.

23.2 Right of Inspection. Within 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 45 calendar days.

23.3 Application. This **Section 23** applies to Contractor, any Affiliate, and any Permitted Subcontractor that performs Services in connection with this Contract.

**24. Support Services.** Contractor will provide the State with the Support Services described in the Service Level Agreement and Support Call Process attached as **Schedule D** to this Contract. Such Support Services will be provided:

**25. Data Security Requirements.** Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will 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 **Schedule E** to this Contract.

**26. Training.** Contractor will provide, at no additional charge, training on the Deliverable provided hereunder in accordance with the times, locations and other terms set forth in a Statement of Work. Upon the State's request, Contractor will timely provide training for additional Authorized Users or other additional training on the Deliverables 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.

## **27. Maintenance Releases; New Versions**

27.1 Maintenance Releases. Provided that the State is current on its Fees, during the Term, Contractor will 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.

27.2 New Versions. Provided that the State is current on its Fees, during the Term, Contractor will 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.

27.3 Reserved.

27.3 Supported Third Party and Open-Source Components. Contractor will utilize only currently supported versions of all Third Party or Open-Source Components and will notify the State when not using the most recently published Third Party and Open-Source Components.

## **28. RESERVED.**

## **29. Contractor Representations and Warranties.**

29.1 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 in accordance with its terms.
- (e) Contractor is neither currently engaged in nor will engage in the boycott of a person based in or doing business with a strategic partner as described in 22 USC 8601 to 8606.

29.2 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 Request for Proposal; 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 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.

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

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

(c) Contractor has, and throughout the Term and any additional periods during which Contractor does or is required to perform the Services will have, the unconditional and irrevocable right, power and authority, including all permits and licenses required, to provide the Services and grant and perform all rights and licenses granted or required to be granted by it under this Contract;

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

(e) 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;

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

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



- (ii) fail to comply with any applicable law;
- (g) as provided by Contractor, the Software does not and will not at any time during the Term contain any:
  - (i) Harmful Code; or
  - (ii) Third party or Open-Source Components that operate in such a way that it is developed or compiled with or linked to any third party or Open-Source Components, other than Approved Third Party Components specifically described in a Statement of Work.
- (h) 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
- (i) Contractor will perform all Services in a 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. In the event of a breach of the foregoing warranty, in addition to any other remedies available to the State under this Contract, Contractor will reperform any nonconforming Services at no cost.
- (k) Contractor acknowledges that the State cannot indemnify any third parties, including but not limited to any third-party software providers that provide software that will be incorporated in or otherwise used in conjunction with the Services, and that notwithstanding anything to the contrary contained in any third-party software license agreement or end user license agreement, the State will not indemnify any third party software provider for any reason whatsoever;
- (l) no Maintenance Release or New Version, when properly installed in accordance with this Contract, will have a material adverse effect on the functionality or operability of the Software.
- (m) all Configurations or Customizations made during the Term will be forward-compatible with future Maintenance Releases or New Versions and be fully supported without additional costs.
- (n) If Contractor Hosted:

(i) Contractor will not advertise through the Hosted Services (whether with adware, banners, buttons or other forms of online advertising) or link to external web sites that are not approved in writing by the State;

(ii) Contractor represents the Software and Services will in all material respects conform to and perform in accordance with the Specifications and all requirements of this Contract, including the Availability and Availability Requirement provisions set forth in the Service Level Agreement;

(iii) all Specifications are, and will be continually updated and maintained so that they continue to be, current, complete and accurate and so that they do and will continue to fully describe the Software in all material respects such that at no time during the Term or any additional periods during which Contractor does or is required to perform the Services will the Software have any material undocumented feature;

(o) During the Term of this Contract, any audit rights contained in any third-party software license agreement or end user license agreement for third-party software incorporated in or otherwise used in conjunction with the Software or with the Hosted Services, if applicable, will apply solely to Contractor or its Permitted Subcontractors. Regardless of anything to the contrary contained in any third-party software license agreement or end user license agreement, third-party software providers will have no audit rights whatsoever against State Systems or networks.

(p) During the term of the Contract, the Software will perform without Defects. If the Software does not perform as warranted, Contractor will use all reasonable efforts, consistent with industry standards, to cure the Defect in accordance with Contractor's then current Support Call Process or to provide State with a functional equivalent.

29.4 Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THIS CONTRACT, CONTRACTOR HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THIS CONTRACT.

**30. Conflicts and Ethics.** Contractor will uphold high ethical standards and is prohibited from: (a) holding or acquiring an interest that would conflict with this Contract; (b) doing anything that creates an appearance of impropriety with respect to the award or performance of the Contract; (c) attempting to influence or appearing to influence any State employee by the direct or indirect offer of anything of value including an offer of employment; or (d) paying or agreeing to pay any person, other than employees and consultants working for Contractor, any consideration contingent upon the award of the

Contract. Contractor must immediately notify the State of any violation or potential violation of these standards. This Section applies to Contractor, any parent, affiliate, or subsidiary organization of Contractor, and any Permitted Subcontractor that provides Deliverables in connection with this Contract.

**31. Compliance with Laws.** Contractor, its subcontractors, including Permitted Subcontractors, and their respective Representatives must comply with all laws in connection with this Contract.

**32. Nondiscrimination.** Under the Elliott-Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, *et seq.*, the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, *et seq.*, and Executive Directive [2019-09](#), Contractor and its 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, partisan considerations, any mental or physical disability, or genetic information that is unrelated to the person's ability to perform the duties of a particular job or position. Breach of this covenant is a material breach of the Contract.

**33. Unfair Labor Practice.** Under MCL 423.324, the State may void this Contract if the name of the Contractor, or the name of a subcontractor, manufacturer, or supplier of the Contractor, subsequently appears on the Unfair Labor Practice register compiled under MCL 423.322.

**34. 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. Contractor waives any objections, such as lack of personal jurisdiction or *forum non conveniens*. Contractor must appoint an agent in Michigan to receive service of process.

**35. Non-Exclusivity.** Nothing contained in this Contract is intended nor is to be construed as creating any requirements contract with Contractor, nor does it provide Contractor with a right of first refusal for any future work. This Contract does not restrict the State or its agencies from acquiring similar, equal, or like Services from other sources.

**36. Force Majeure**

36.1 Force Majeure Events. 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.

36.2 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 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.

36.3 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 Hosted Services 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 Hosted Services; or

(ii) 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.

(b) no Force Majeure Event modifies or excuses Contractor’s obligations under **Section 21** (State Data), **22** (Non-Disclosure of Confidential Information), or **17** (Indemnification) of the Contract, Disaster Recovery and Backup requirements set forth in the Service Level Agreement, or any data retention or security requirements under the Contract.

**37. Dispute Resolution.** The parties will endeavor to resolve any Contract dispute in accordance with this provision. The dispute will be referred to the parties' respective Contract Administrators or Program Managers. Such referral must include a description of the issues and all supporting documentation. The parties must submit the dispute to a senior executive if unable to resolve the dispute within 20 business days. The parties will continue performing while a dispute is being resolved, unless the dispute precludes performance. A dispute involving payment does not preclude performance. Litigation to resolve the dispute will not be instituted until after the dispute has been elevated to the parties' senior executive and either concludes that resolution is unlikely or fails to respond within 20 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 does not limit the State's right to terminate the Contract.

**38. 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.

**39. Severability.** If any part of this Contract is held invalid or unenforceable, by any court of competent jurisdiction, that part will be deemed deleted from this Contract and the severed part will be replaced by agreed upon language that achieves the same or similar objectives. The remaining Contract will continue in full force and effect.

**40. Waiver.** Failure to enforce any provision of this Contract will not constitute a waiver.

**41. Survival.** Any right, obligation, or condition that, by its express terms or nature and context is intended to survive, will survive the termination or expiration of this Contract; such rights, obligations, or conditions include, but are not limited to, those related to transition responsibilities; indemnification; disclaimer of damages and limitations of liability; State Data; non-disclosure of Confidential Information; representations and warranties; insurance and bankruptcy.

**42. Administrative Fee and Reporting.** Contractor must pay an administrative fee of 1% on all payments made to Contractor under the Contract for transactions with MiDEAL members, and other states (including governmental subdivisions and authorized entities). For clarity, Contractor will not be obligated to pay the 1% administrative fee for payments to the Contractor under the Contract for transactions

with the State itself. Administrative fee payments must be made online by check or credit card at: <https://www.thepayplace.com/mi/dtmb/adminfee>

Contractor must submit an itemized purchasing activity report, which includes at a minimum, the name of the purchasing entity and the total dollar volume in sales. Reports should be mailed to [MiDeal@michigan.gov](mailto:MiDeal@michigan.gov).

The administrative fee and purchasing activity report are due within 30 calendar days from the last day of each calendar quarter.

**43. Extended Purchasing Program.** This contract is extended to MiDEAL members. MiDEAL members include local units of government, school districts, universities, community colleges, and nonprofit hospitals. A current list of MiDEAL members is available at [www.michigan.gov/mideal](http://www.michigan.gov/mideal).

Upon written agreement between the State and Contractor, this contract may also be extended to: (a) other states (including governmental subdivisions and authorized entities) and (b) State of Michigan employees.

If extended, Contractor must supply all Contract Activities at the established Contract prices and terms. The State reserves the right to impose an administrative fee and negotiate additional discounts based on any increased volume generated by such extensions.

Contractor must submit invoices to, and receive payment from, extended purchasing program members on a direct and individual basis.

**44. Contract Modification.** This Contract may not be amended or modified in any way, except by a properly signed **Change Notice**. Notwithstanding the foregoing, no subsequent Statement of Work or Change Notice executed after the Effective Date will be construed to amend this Contract unless it specifically states its intent to do so and cites the section or sections amended.

**45. Reserved.**

**46. Accessibility Requirements.**

46.1 Except for Software provided by Contractor under this Contract exclusively for use by State employees only, all Software provided by Contractor under this Contract, including associated content and documentation, must at all times conform to the Digital Accessibility Standards. Throughout the Term of the Contract, Contractor must:

- (a) maintain compliance with the Digital Accessibility Standards;
- (b) comply with plans and timelines approved by the State to achieve conformance in the event of any deficiencies;
- (c) ensure that no Maintenance Release, New Version, update or patch, when properly installed in accordance with this Contract, will have any adverse effect on the conformance of Contractor's Software to the Digital Accessibility Standards;
- (d) promptly respond to and resolve any complaint the State receives regarding accessibility of Contractor's Software;
- (e) upon the State's written request, provide evidence of compliance with this Section by delivering to the State Contractor's most current PAT for each product provided under the Contract; and
- (f) participate in the State of Michigan Digital Standards Review described below.

46.2 State of Michigan Digital Standards Review. Throughout the Term, Contractor must assist the State, at no additional cost, with development, completion, and on-going maintenance of an accessibility plan, which requires Contractor, upon request from the State, to submit evidence to the State to review and validate Contractor's accessibility and compliance with the Digital Accessibility Standards. Prior to the solution going-live an assessment is required, and thereafter on an annual basis, or as otherwise required by the State, re-assessment of accessibility may be required. At no additional cost, Contractor must remediate all issues identified from any assessment of accessibility pursuant to plans and timelines that are approved in writing by the State.

46.3 Warranty. Contractor warrants that all conformance claims regarding conformance to the Digital Accessibility Standards made by Contractor pursuant to this Contract, including all information provided in any PAT Contractor provides to the State, are true and correct. If the State determines such conformance claims provided by the Contractor represent a higher level of conformance than what is actually provided to the State, Contractor will, at its sole cost and expense, promptly remediate its Software to align with Contractor's stated conformance claims in accordance with plans and timelines that are approved in writing by the State. If Contractor is unable to resolve such issues in a manner acceptable to the State, in



addition to all other remedies available to the State, the State may terminate this Contract for cause under **Subsection 16.1**.

46.4 Contractor must, 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 arising out of its failure to comply with the foregoing accessibility standards.

46.5 Failure to comply with the requirements in this **Section 46** shall constitute a material breach of this Contract.

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

**48. Relationship of the Parties.** The relationship between the parties is that of independent contractors. Contractor, its employees, and agents will not be considered employees of the State. No partnership or joint venture relationship is created by virtue of this Contract. Contractor, and not the State, is responsible for the payment of wages, benefits and taxes of Contractor's employees and any subcontractors. Prior performance does not modify Contractor's status as an independent contractor. Neither party has authority to contract for nor bind the other party in any manner whatsoever.

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

**50. 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.

**51. 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 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.

**52. 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 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 Deliverables. Without limiting the generality of the foregoing, Contractor acknowledges and agrees that, if Contractor or its estate will 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 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.

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

<b>Schedule A</b>	Statement of Work
<b>Schedule B</b>	Pricing Schedule
<b>Schedule C</b>	Insurance Schedule
<b>Schedule D</b>	Service Level Agreement
<b>Schedule E</b>	Data Security Requirements
<b>Schedule E, Att. 1</b>	Criminal Justice Information Services
<b>Schedule E, Att. 2</b>	Vulnerability Remediation Timeframe (VRT)

**Schedule F**

**Disaster Recovery Plan**

**54. 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.

**55. ENTIRE AGREEMENT. THESE TERMS AND CONDITIONS, INCLUDING ALL STATEMENTS OF WORK AND OTHER SCHEDULES AND EXHIBITS (AGAIN COLLECTIVELY THE “CONTRACT”) 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 TERMS AND CONDITIONS, THE SCHEDULES, EXHIBITS, AND A STATEMENT OF WORK, THE FOLLOWING ORDER OF PRECEDENCE GOVERNS: (A) FIRST, THESE TERMS AND CONDITIONS AND (B) SECOND, SCHEDULE E – DATA SECURITY REQUIREMENTS AND (C) THIRD, EACH STATEMENT OF WORK; AND (D) FOURTH, THE REMAINING EXHIBITS AND SCHEDULES TO THIS CONTRACT. NO TERMS ON CONTRACTOR’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, EVEN IF ATTACHED TO STATE’S DELIVERY OR PURCHASE ORDER, WILL CONSTITUTE A PART OR AMENDMENT OF THIS CONTRACT OR IS BINDING ON THE STATE OR ANY AUTHORIZED USER FOR ANY PURPOSE. ALL SUCH OTHER TERMS AND CONDITIONS HAVE NO FORCE AND EFFECT AND ARE DEEMED REJECTED BY THE STATE 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**

This schedule identifies the requirements of this Contract.

### **1. DEFINITIONS**

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

<b>Term</b>	<b>Definition</b>
ATO	Authorization to Operate. Must be obtained from Michigan Cyber Security before system is allowed to go live.
AVL	Automatic Vehicle Location. Mapping technology that uses GIS to locate and show Trooper vehicle locations on a map.
CAD	Computer Aided Dispatch software used by dispatchers to track all calls and first responder's locations/activity. (the Management information system)
CJI	Criminal Justice Information subject to FBI's CJIS Security Policy requirements, and includes all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws.
CJIS	Criminal Justice Information Services. FBI standards to protect highly sensitive and restricted data.
CHRI	Criminal History Record Information is a subset of CJI subject to FBI's CJIS Security Policy requirements.
EASA	Enterprise Architecture Solutions Assessment. Network drawings and assessment of solution needed as part of the System Security Plan.
EMD	Emergency Medical Dispatch software that allows dispatcher to input symptoms and get medical advice to give to caller.
EMS	Emergency Medical Services (like ambulances).

ENS	Emergency Notification Solution. Emergency Alert system utilized to send out notifications in emergencies.
GIS	Geographic Information System. Type of mapping technology.
GPS	Global Positioning Satellite. Used to display and track locations on a map.
LEIN	Law Enforcement Information Network. Contains Personal identifying information (PII) and CJI.
MCS or MC3	Michigan Cyber Security. Regulates all security for any system that touches the State of Michigan network system.
MDC	Mobile Data Computers. Rugged Laptops in the field that Troopers use in their cars. Can remove from docks in the cars.
MDOT	Michigan. Department of Transportation. Has pole cameras around the state that can be accessed to see activity/accidents on the road.
MIS	Management Information System. System that tracks information from voice and radio calls.
MPSCS	Michigan Public Safety Communications System. Houses and administers current CAD that MSP utilizes. Also houses the 800 Mhz Radio System the State of Michigan uses for first responders.
MSP	The Michigan State Police
NICE	Vendor software currently used by MSP to record, store and playback all 911 calls based on retention schedules.
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
Premier One	Motorola CAD system that MSP currently uses.

ProQA	Current EMD software used by MSP current 911 phone system
PSAP	Public Safety Answering Points. A 911 center that is the first point of contact (answering) from a person calling 911 is a PSAP. There are secondary PSAP that would be a back-up or main function is other dispatch duties but not first contact from 911 caller.
RCC	Regional Communication Center are what MSP calls their 911 dispatch centers.
SaaS	Software-as-a-Service
SOLUTION	Deliverables (including but not limited to Software, Hardware, and Documentation) and Services (including but not limited to Hosting Services, Support Services), singularly or in any combination thereof as set forth in a Statement of Work intended to address the State's needs.
SOM	State of Michigan
SSP	System Security Plan. Part of the overall assessment conducted to obtain an authority to operate.

## 2. BACKGROUND

MSP Emergency Dispatchers are 911 dispatchers for first responders around the State of Michigan including State Troopers. CAD is the system used to record incidents from 911 calls and Trooper check ins. The information sometimes ties to the SOM LEIN system. It also ties to the SOM 800 Mhz radio system. Other ties it may have would be to various web next generation programs that offer things like ability for callers to show live footage from scene, ProQA (emergency medical dispatch software), and extensive GIS mapping/AVL features. The current CAD is on premise (through MPSCS) but the desire is for the new CAD system to be Contractor hosted/SaaS maintained.

Since Troopers are stationed all around the State of Michigan, they interact with numerous Emergency Dispatch centers around the State. Currently each center uses a different vendor for their CAD. Some CAD's talk to each other, while some don't have that capability. Having a CAD system that allows MSP dispatchers/troopers to interact with all CADs is critical for doing their duties.

### 3. PURPOSE

Contractor is providing a Contractor Hosted Software Solution and applicable Services to replace the MSP existing CAD system. Contractor's CAD system has a next generation feature and will be able to interact with all CAD systems utilized by MSP dispatchers/troopers in order to improve communications for the first responders and dispatch centers.

### 4. IT ENVIRONMENT RESPONSIBILITIES

Included in Schedule E – Data Security Requirements; the Contractor will be required to meet all State Policy Standards and Procedures (PSP's), public and non-public applicable to this Contract.

Refer to Schedule F for Contractor's Disaster Recovery Plan.

#### **For a Contractor Hosted Software Solution:**

##### **Definitions:**

**Facilities** – Physical buildings containing Infrastructure and supporting services, including physical access security, power connectivity and generators, HVAC systems, communications connectivity access and safety systems such as fire suppression.

**Infrastructure** – Hardware, firmware, software, and networks, provided to develop, test, deliver, monitor, manage, and support IT services which are not included under Platform and Application.

**Platform** – Computing server software components including operating system (OS), middleware (e.g., Java runtime, .NET runtime, integration, etc.), database and other services to host applications.

**Application** – Software programs which provide functionality for end user and Contractor services.

**Storage** – Physical data storage devices, usually implemented using virtual partitioning, which store software and data for IT system operations.

**Backup** – Storage and services that provide online and offline redundant copies of software and data.

**Development** - Process of creating, testing and maintaining software components.

<b>Component Matrix</b>	Identify contract components with contractor and/or subcontractor name(s), if applicable
Facilities	AWS GovCloud
Infrastructure	AWS GovCloud
Platform	Microsoft
Application	Tyler Technologies
Storage	AWS GovCloud
Backup	AWS GovCloud
Development	Tyler Technologies

The deployment utilizes Microsoft Windows Server 2022 to host the applications and SQL Server 2022 for the databases. The Microsoft licensing is included in the annual SaaS fee. Contractor staff is responsible for provisioning, maintaining and updating the Microsoft components.

## 5. ADA COMPLIANCE

The State is required to comply with the Americans with Disabilities Act of 1990 (ADA) and has adopted standards and procedures regarding accessibility requirements for websites and software applications. Except for Software provided by Contractor under this Contract exclusively for use by State employees only, all websites, applications, software, and associated content and documentation provided by the Contractor as part of the Solution must comply with the Digital Accessibility Standards.

## 6. USER TYPE AND CAPACITY

Type of User	Access Type	Number of Users	Number of Concurrent Users
In House Technical Support	Admin	8	6
Dispatchers	Write Access	82	35
Supervisors or Lead	Lead/Supervisor Access	12	10
Troopers	Write Access	2,000	995

Contractor Solution must meet the expected number of concurrent Users.





Contractor must support the current and future State standard environment at no additional cost to the State.

## **10. SOFTWARE**

Software requirements are identified in **Schedule A – Table 1 Business Specification Worksheet**.

Contractor must provide a list of any third party components, and open source component included with or used in connection with the deliverables defined within this Contract. This information must be provided to the State on a quarterly basis and/or if a new third party or open source component is used in the performance of this Contract.

### **Look and Feel Standards**

All software items provided by the Contractor must adhere to the State of Michigan Application/Site standards which can be found at <https://www.michigan.gov/standards>.

### **Mobile Responsiveness**

If the software will be used on a mobile device as define in Schedule A – Table 1, Business Specification Worksheet, the Software must utilize responsive design practices to ensure the application is accessible via a mobile device.

### **SOM IT Environment Access**

Contractor must access State environments using one or more of the following methods:

- State provided VDI (Virtual Desktop Infrastructure) were compliant.
- State provided and managed workstation device.
- Contractor owned and managed workstation maintained to all State policies and standards.
- Contractor required interface with State systems which must be maintained in compliance with State policies and standards as set forth in **Schedule E – Data Security Requirements**.

Contractor must access State environments from locations within the continental United States.

Below are the Contractor's identified third-party components, including open source components included with or used in connection with the proposed solution.

Embedded third-party software (ArcGIS Enterprise, GIS Server Role, and Extensions previously known as ArcGIS Server advanced)

## **11. INTEGRATION**

Contractor must integrate their solution to the following technologies:

Current Technology	Current Motorola 911 Phone System.
Volume of Data	Data is a live feed from 911 phone system.
Format of the input & export files	N/A

Current Technology	Automatic Vehicle Location (AVL)
Volume of Data	GIS/GPS mapping technology, live feeds of real time location of Trooper vehicles, boats, planes, etc.
Format of the input & export files	N/A

Current Technology	Automatic Vehicle Location (AVL)
Volume of Data	GIS/GPS mapping technology, live feeds of real time location of Trooper vehicles, boats, planes, etc.
Format of the input & export files	N/A

Current Technology	Motorola – 800 MHz radio system (via MPSCS)
Volume of Data	Data is a live feed with radio system

Format of the input & export files	N/A
------------------------------------	-----

Current Technology	Rapid SOS
Volume of Data	Live feed with this cloud based vendor that allows for various 911 next generation location features.
Format of the input & export files	N/A

Current Technology	LEIN (NCIC) (INLETS)
Volume of Data	Live feed to the State's LEIN network for live updates on vehicle and person information
Format of the input & export files	N/A

Current Technology	ProQA – Emergency Medical Dispatch
Volume of Data	3 <sup>rd</sup> party vendor that is used to help asses and give medical advice to 911 medical need calls.
Format of the input & export files	N/A

## 12. MIGRATION

Contractor must migrate the data identified in the table below:

Current Technology	Motorola Premier 1 Mobile CAD
Data Format relative to the database technology used.	Need data for 1 year, to fulfill retention schedule.
Number of data fields to give Contractor awareness of the size of the schema.	Unknown
Volume of Data	Unknown
Database current size.	Unknown

The database may be increased at the time of transition, if required by the State.

## 13. RESERVED.

## 14. TRAINING SERVICES

The Contractor must provide administration and end-user training for implementation, other training, go-live support, and transition to customer self-sufficiency. Contractor to provide a comprehensive training plan as part of its overall implementation plan that will be reviewed and approved by the State. The plan will define a detailed course of action to guide the progress of the project training for the system. The plan will include course outlines, proposed schedules, location of the training, recommended and required attendees, hardware requirements and methodology of instruction.

Training numbers:

Participants	Estimated Number of Users to be Trained	Frequency	Additional Information
*End User Training	10 # Classroom (dispatchers)	At least 6 different in-person training events for End Users prior to go-live. Availability for	Hybrid of classroom with e-learning/online option

		1 additional End User Training per year for duration of contract.	
*Administrative User Training	10 # Classroom	At least 2 Train the Trainer events in person per year.	Classroom (in person)
*Other User Training	500 # e-learning/online (future training for new hires)	E-learning/online training catalog with video and handouts to help with future hires.	On-line manuals and pre-recorded video training guides to be provided for future onboarding.
Mobile Training	60 # Trainers	Train the Trainer with eLearning and Video Training	Video and eLearning as a supplement to in-person Train the Trainer.

\*Location of trainings will vary throughout the State. Additionally, MSP reserves the right to change frequency of trainings.

## 15. RESERVED

## 16. DOCUMENTATION

Contractor must provide all 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.

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.

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.

## 17. ADDITIONAL PRODUCTS AND SERVICES

## 18. CONTRACTOR PERSONNEL

**Contractor Contract Administrator.** Contractor resource who is responsible to (a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

Contractor
<b>Name:</b> Andrew B Hittle, President Public Safety Division <b>Address:</b> 840 West Long Lake Road, Troy, Michigan 48909 <b>Phone:</b> 248-269-1000 <b>Email:</b> Andrew.Hittle@tylertech.com

**Contractor Security Officer.** Contractor resource who is responsible to respond to State inquiries regarding the security of the Contractor's Solution. This person must have sufficient knowledge of the security of the Contractor Solution and the authority to act on behalf of Contractor in matters pertaining thereto. Contractor must inform the State of any change to this resource.

Contractor
<b>Name:</b> Jeremy Ward, CISO <b>Address:</b> One Tyler Drive, Yarmouth, Maine 04096 <b>Phone:</b> 800-772-2260 <b>Email:</b> Jeremy.Ward@tylertech.com

## 19. CONTRACTOR KEY PERSONNEL

**Contractor Project Manager.** Contractor resource who is responsible to 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, matters pertaining to the receipt and processing of Support Requests and the Support Services.

Contractor
<b>Name:</b> Elizabeth Des Meules <b>Address:</b> 840 West Long Lake Road Troy, Michigan 48098 <b>Phone:</b> (248) 269-1000, ext. 1985 <b>Email:</b> Elizabeth.DesMeules@tylertech.com

## 20. CONTRACTOR PERSONNEL REQUIREMENTS

**Background Checks.** Contractor must present certifications evidencing satisfactory ICHAT for all staff identified for assignment to this project to the State of Michigan Program Manager designated for this Contract. In addition, proposed

Contractor personnel will be required to complete a Michigan State Police background check and/or submit an RI-8 Fingerprint Card for the National Crime Information Center (NCIC), if required by project.

Annually, the State may perform an ICHAT for all staff identified for assignment to this project. Annual background check results will be reported to the State of Michigan Program Manager designated for this Contract.

Contractor personnel must follow MSP's background check process if coming on site to perform work.

Contractor, while employed with DTMB, will disclose to the State of Michigan Program Manager for this Contract, in writing at or before the beginning of the next scheduled duty shift:

- a. A felony or misdemeanor court conviction, whether by guilty plea, no contest plea or trial.
- b. A felony arraignment.
- c. Restriction, suspension, or loss of driving privileges for any reason, if the employee's current position requires possession of a valid driver's license.

Contractor will pay for all costs associated with ensuring its staff meet all requirements.

Contractor must notify the State Program Manager(s) prior to removing or replacing any Contractor Personnel with access to State Data under this Contract. Contractor must also provide written certification to the State Program Manager(s) that Contractor Personnel's access to State Data has been terminated. Contractor must notify the State in advance of allocating Contractor Personnel to multiple State Contracts or Projects (discuss timeframe for notification). Contractor must provide detail of how a given Contractor Personnel meets the resource experience requirements in advance of replacing a Contractor Personnel. Contractor must provide monthly summary of Contractor Personnel allocation for all Contractor Personnel who have access to State Data.

Contractor must seek approval from the State prior to removing or replacing any Contractor Personnel with access to State Data.

**Contractor Resources.** Contractor Personnel must be located in the continental United States, per the Schedule E – Data Security Requirements. Contractor must comply with the data security and other requirements in this Contract.

**Disclosure of Subcontractors.**

AWS is a Permitted Subcontractor.

If the Contractor intends to utilize subcontractors, the Contractor must disclose the following:

- The legal business name; address; telephone number; a description of subcontractor's organization and the services it will provide; and information concerning subcontractor's ability to provide the Contract Activities.
- The relationship of the subcontractor to the Contractor.
- Whether the Contractor has a previous working experience with the subcontractor. If yes, provide details of that previous relationship.
- A complete description of the Contract Activities that will be performed or provided by the subcontractor.

## 21. STATE RESOURCES/RESPONSIBILITIES

The State will provide the following resources as part of the implementation and ongoing support of the Solution.

**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.

<b>State Contract Administrator</b>
-------------------------------------

<b>Name:</b> Kristine Mills <b>Phone:</b> 517-242-6402 <b>Email:</b> millsk11@michigan.gov
--

**Program Managers.** The DTMB and Agency Program Managers (or designee) will jointly approve all Deliverables and day to day activities.

<b>DTMB Program Manager</b>
-----------------------------

<b>Name:</b> Jim Coggins <b>Phone:</b> 517-243-5265 <b>Email:</b> cogginj@michigan.gov
--

<b>Agency Program Manager</b>
-------------------------------

<b>Name:</b> Jonathon Whitford <b>Phone:</b> 517-512-4068 <b>Email:</b> whitfordj@michigan.gov
--

## 22. MEETINGS

At start of the engagement, the Contractor Project Manager must facilitate a project kick off meeting with the support from the State's Project Manager and the identified State



resources to review the approach to accomplishing the project, schedule tasks and identify related timing, and identify any risks or issues related to the planned approach. From project kick-off until final acceptance and go-live, Contractor Project Manager must facilitate weekly meetings (or more if determined necessary by the parties) to provide updates on implementation progress. Following go-live, Contractor must facilitate monthly meetings (or more or less if determined necessary by the parties) to ensure ongoing support success.

The State reserves the right to request other meetings as it deems appropriate. Contractor personnel may be responsible for attending, planning and facilitating such meetings.

### **23. PROJECT CONTROL & REPORTS**

Once the Project Kick-Off meeting has occurred, the Contractor Project Manager will monitor project implementation progress and report on a weekly basis to the State's Project Manager the following:

- Progress to complete milestones, comparing forecasted completion dates to planned and actual completion dates
- Accomplishments during the reporting period, what was worked on and what was completed during the current reporting period
- Indicate the number of hours expended during the past week, and the cumulative total to date for the project. Also, state whether the remaining hours are sufficient to complete the project
- Tasks planned for the next reporting period
- Identify any existing issues which are impacting the project and the steps being taken to address those issues
- Identify any new risks and describe progress in mitigating high impact/high probability risks previously identified
- Indicate the amount of funds expended during the current reporting period, and the cumulative total to date for the project.

All Contractors must submit and enter weekly timesheets into the State of Michigan's Project Portfolio Management tool, Clarity PPM, for approval and reporting. The weekly Clarity PPM timesheet will contain hours worked for assigned project tasks.

### **24. PROJECT MANAGEMENT**

The Contractor Project Manager will be responsible for maintaining a project schedule (or approved alternative) identifying tasks, durations, forecasted dates and resources – both Contractor and State - required to meet the timeframes as agreed to by both parties.

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 parties to the change and clearly identify the impact to the overall project.

### **SUITE Documentation**

In managing its obligation to meet the above milestones and deliverables, the Contractor is required to utilize the applicable [State Unified Information Technology Environment \(SUITE\)](#) methodologies, or an equivalent methodology proposed by the Contractor.

#### Milestones/Deliverables for Implementation

The proposed milestones and associated deliverables are set forth below.

Milestone Event	Associated Milestone Deliverable(s)	Schedule	Payment
Stage 1 - Initiate & Plan	<ul style="list-style-type: none"> <li>- Project Management Plan</li> <li>- Initial Project Schedule</li> <li>- Stakeholder Meeting</li> </ul>	1.6 - Control Point 1: Initiate & Plan Stage Acceptance	10%
Stage 2 - Access & Design	<ul style="list-style-type: none"> <li>- Documentation of future state decisions and configuration options to support future state decisions.</li> <li>- Custom Interface specification document(s).</li> <li>- Conversion plan built.</li> </ul>	2.6 - Control Point 2: Assess & Define Stage Acceptance	10%
Stage 3 - Prepare Solution	<ul style="list-style-type: none"> <li>- Licensed software is installed.</li> <li>- Installation checklist/system document.</li> <li>- Conversion iterations and reviews complete.</li> <li>- Completed Custom Interfaces.</li> </ul>	3.7 - Control Point 3: Prepare Solution Stage Acceptance	20%
Stage 4 - Production Readiness	<ul style="list-style-type: none"> <li>- Solution Validation Report.</li> <li>- Update go-live action plan and checklist.</li> <li>- End user training.</li> </ul>	4.4 - Control Point 4: Production Readiness Stage Acceptance	25%

Stage 5 - Production	- Live in Production - Post Go Live Report.	5.4 - Control Point 5: Production Stage Acceptance	25%
Stage 6 - Close	- Post Project Report.	6.3 - Control Point 6: Close Stage Acceptance	10%

*ATO must be accepted prior to go live. This may delay actual go live date.*

Below is the Contractor's Work Breakdown Structure (WBS)

The Work Breakdown Structure (WBS) is a hierarchical representation of the Project broken down into smaller, more manageable components. The top-level components are called "Stages" and the second level components are called "Work Packages". The work packages, shown below each stage, contain the high-level work to be done. The detailed Project Schedule, developed during Project/Phase Planning and finalized during subsequent stages, lists the tasks to be completed within each work package. Each stage ends with a "Control Point", confirming the work performed during that stage of the Project has been accepted by the State.

1. Initiate & Plan	2. Assess & Define	3. Prepare Solution	4. Production Readiness	5. Production	6. Close
1.1 Initial Coordination	2.1 Solution Orientation	3.1 Initial System Deployment	4.1 Solution Validation	5.1 Go Live	6.1 Phase Close Out
1.2 Project/Phase Planning	2.2 Current & Future State Analysis	3.2 Configuration	4.2 Go Live Readiness	5.2 Transition to Client Services	6.2 Project Close Out
1.3 GIS Planning*	2.3 Modification Analysis	3.3 Process Refinement	4.3 End User Training	5.3 Post Go Live Activities	
1.4 Infrastructure Planning	2.4 Conversion Assessment	3.4 Conversion Delivery			
1.5 Stakeholder Meeting	2.5 Data Assessment	3.5 Data Delivery			
		3.6 Modification Delivery			
1.6 Control Point Stage 1	2.6 Control Point Stage 2	3.7 Control Point Stage 3	4.4 Control Point Stage 4	5.4 Control Point Stage 5	6.3 Control Point Stage 6

The following process will be used for accepting Deliverables and Control Points:

- The State shall have ten (10) business days from the date of delivery, or as otherwise mutually agreed upon by the parties in writing, to accept each Deliverable or Control Point. If the State does not provide acceptance or acknowledgement within ten (10) business days, or the otherwise agreed upon timeframe, not to be unreasonably withheld, Contractor deems the Deliverable or Control Point as accepted.
- If the State does not agree the Deliverable or Control Point meets requirements, the State shall notify Contractor project manager(s), in writing, with reasoning within ten (10) business days, or the otherwise agreed-upon timeframe, not to be unreasonably withheld, of receipt of the Deliverable.
- Contractor shall address any deficiencies and redeliver the Deliverable or Control Point within 30 days of the written notice from the State. The State shall then have ten (10) business days from receipt of the redelivered Deliverable or Control Point to accept or again submit written notification of reasons for rejecting the milestone. If the State does not provide acceptance within ten (10) business days, or the otherwise agreed upon timeframe, not to be unreasonably withheld, Contractor deems the Deliverable or Control Point as accepted.

### **Control Point 1: Initiate & Plan Stage Acceptance**

#### Initiate & Plan Stage Deliverables:

- Project Management Plan
- Initial Project Schedule

#### Initiate & Plan stage acceptance criteria:

- All stage deliverables accepted based on acceptance criteria defined
- Project governance defined
- Project portal made available to the State
- Stakeholder meeting complete
- GIS Data Production Ready
- Completed Infrastructure Requirements and Design Document
- System Passes Infrastructure Audit (as applicable)

### **Control Point 2: Assess & Define Stage Acceptance**

#### Assess & Define Stage Deliverables:

- Documentation of future state decisions and configuration options to support future state decisions.
- Modification specification document.

#### Assess & Define Stage Acceptance Criteria:

- All stage deliverables accepted based on criteria previously defined.
- Solution Orientation is delivered.
- Conversion data extracts are received by Contractor.
- Data conversion plan built.

### **Control Point 3: Prepare Solution Stage Acceptance**

#### Prepare Solution Stage Deliverables:

- Licensed software is installed or made available via Cloud.
- Installation checklist/system document.
- Conversion iterations and reviews complete.
- Completed modifications.
- Revised configuration for modification (if applicable).

#### Prepare Solution Stage Acceptance Criteria:

- All stage deliverables accepted based on criteria previously defined.
- Software is configured.

### **Control Point 4: Production Readiness Stage Acceptance**

#### Production Readiness stage deliverables:

- Solution Validation Report.
- Update go-live action plan and/or checklist.
- End user training.

#### Production Readiness stage acceptance criteria:

- All stage deliverables accepted based on criteria previously defined.
- Go-Live planning session conducted.

### **Control Point 5: Production Stage Acceptance**

#### Production Stage deliverables:

- Converted data is available in cloud archive environment.

#### Production Stage Acceptance Criteria:

- All stage deliverables accepted based on criteria previously defined.
- Go-Live activities defined in the Go-Live action plan completed.
- Client services support document is provided.

## **Control Point 6: Close Stage Acceptance**

### Close Stage Deliverables:

- Post Project Report.

### Close Stage Acceptance Criteria:

- Completed report indicating all Project deliverables and milestones have been completed.
- Final System Acceptance Test, as described below, has been met.

## **Final Software Acceptance Test**

Final Software Acceptance Test is intended to verify that the Software contracted by the State and delivered by Contractor meets reliability requirements in accordance with the Agreement between the parties. Any such process must provide that final acceptance will be issued when the Contractor Software operates in live production without Priority Level 1 or 2 Defects, as defined in the Support Call Process, for 30 consecutive days.

If any Priority Level 1 or 2 Defects, as agreed on by the State and Contractor, are discovered during the 30-day period, Contractor will resolve such Defects in accordance with the Support Call Process and the 30-day time period will reset.

Final Software Acceptance Tests are performed in the State's live production environment.

## **25. ADDITIONAL INFORMATION**

As of the Effective Date, there is no Work Product included under this Contract.

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

Public Safety Analytics (Citizen Connect) is a publicly accessible part of the Software that is not exclusively for use by State employees only and must comply with the Digital Accessibility Standards.

## SCHEDULE A – TABLE 1 – BUSINESS SPECIFICATION WORKSHEET

---

The Business Specifications Worksheet contains columns and is defined as follows:

**Column A:** Business Specification number.

**Column B:** Business Specification description.

**Column C:** Contractor's indication of how it will comply with the business Specification.

- **Current Capability** – This capability is available in the proposed Solution with no additional configuration or cost
- **Requires Configuration** – This capability can be met through Contractor-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).
- **Customizations to Software Required** – The requirement can be met through Contractor modifying the underlying source code, which can be completed as part of the initial implementation.
- **Future Enhancement** – This capability is a planned enhancement to the base software and will be available within the next 12 months of contract execution at no additional cost.
- **Not Available** – This capability is not currently available, and a future enhancement is not planned.

**NOTE:** Configuration is referred to as a change to the Solution that must be completed by the awarded 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).

Customization is referred to a modification to the Solution's underlying source code, which can be completed as part of the initial implementation. All configuration changes or customization modifications made during the term of the awarded contract must be forward-compatible with future releases and be fully supported by the awarded Contractor without additional costs.

A	B	C				
Business Specification Number	Business Specification	Current Capability	Requires Configuration	Requires Customization	Future Enhancement	Not Available
<b>REQUIRED</b>						
1.0	Contractor must have a system that can serve 4 MSP dispatch centers running simultaneously with up to 35 dispatchers dispatching for over 130 areas.	Y				
2.0	MSP CAD system will require up to 1,075 concurrent licenses. Estimated no more than 1,075 would be used at any given time. <ul style="list-style-type: none"> <li>Will need 955 for Mobile Data Computers (MDC) in the field (Troopers use).</li> <li>Will need 35 for all Dispatch consoles at the 4 MSP Dispatch Centers.</li> </ul>	Y				



	<ul style="list-style-type: none"> <li>Will need 75 test environment licenses for Recruit School.</li> <li>Will need 10 administrative level including test environment licensing for in-house CAD Administrators.</li> </ul>					
3.0	24/7 x 365 days Customer Support/Maintenance via Phone and offer leveraging remote access to CAD system for complete resolution methods. Accepting calls from both Dispatchers and Troopers.	Y				
4.0	Ability to request support via email if MSP staff feel issue doesn't need immediate attention.	Y				
5.0	System must have a type of customer support portal, where system problems can be reported and tracked.	Y				
6.0	Contractor to have customer support contact (single contact) who will maintain regular communications with MSP and will continually monitor and assess MSP services delivered.	Y				
7.0	Provide regular status updates of problem resolution and escalated incidents.	Y				
8.0	Level of Response Times based on severity of problem. <b>Critical:</b> 1 or more functions are unavailable, or no longer working. Full	Y				

	<p>System Outage. Response time should be within 1 hour of notification.</p> <p><b>High:</b> Function is unavailable, so normal business activity is impacted or decreased. Work around may be available; however, efficiency is degraded. Response time should be within 3 hours.</p> <p><b>Medium:</b> Functions available; however, there is deviation from expected service. Response time should be within 8 hours.</p> <p><b>Low or Minor:</b> minor issues, cosmetic issues, general usage questions, configuration questions. Response time should be within 2 days.</p>					
9.0	Contractor will provide trained technical resources who have passed an MSP background check to work on product onsite (MSP) when necessary or when remote accessing infrastructure.	Y				
10.0	Contractor will execute software upgrades as they become available. Offering a test environment for MSP to test prior to going live with update.	Y				
11.0	Product updates that provide enhanced/new features should be outlined to MSP at time of release of new update. MSP should have option to review new/enhanced features prior to updating software.	Y				
12.0	Updates to software must be implemented on the system within 2 months of update release or be	Y				

	implemented prior to the next software update release, whichever comes first. Any delay from this must be approved by business owner.					
13.0	Contractor will maintain industry standard security measures to protect the CAD from intrusion, breach, corruption, or security risks.	Y				
14.0	Contractor and Software must comply with FBI defined Criminal Justice Information Services (CJIS) Security Policy/Standards.	Y				
15.0	Software must comply with National Institute of Standards and Technology (NIST) Standards.	Y				
16.0	Contractor must comply with all requests from MSP security teams to gather necessary Contractor information (like SOC reports) to achieve an Authority to Operate (ATO) from the State of Michigan Security Team, prior to going live.	Y				
17.0	System needs to provide accurate, timely, and secure information to dispatchers and officers in the field with real time updates as Dispatcher or Trooper updates incident.	Y				
18.0	Back-up offline feature where if network connectivity is lost, the system must have ability to continue to operate allowing Dispatchers and Troopers ability to enter information on incidents, then once network is available again,	Y				

	system has ability to update information entered so it is all synced again.					
19.0	System must provide single or multi-jurisdictional dispatching for law enforcement, fire, and EMS.	Y				
20.0	System must be integrated with real time GIS (open source) mapping updates. Ability to see different open-source views like street view, satellite view, etc.	Y				
21.0	System must have accurate mile marker and location verification.	Y				
22.0	System must have ability to have alternate names (like a landmark name) tied to a specific GPS location. So, if dispatcher types the “the blue bridge or Great America Park” they know where the person is on the map. Alternate names should not be dependent on capitalization or misspelling.	Y				
23.0	System must have ability to have location comments, special locations (landmarks, common places), history, and advisories.	Y				
24.0	System must have ability to have “sound alike” location verification in the mapping feature. Example: if someone spells “Soo Sainte Marie” system would find and input “Sault Ste. Marie”	Y				
25.0	Mapping feature should have ability to geo fence an area on the map to find specific address or business to a defined area. Example: if you type	Y				

	McDonalds, system shows you the McDonalds in the specific area you are dispatching for, not the entire list of McDonalds in the State.					
26.0	Mapping feature should have ability to differentiate a city based on address. Example: if caller says they live at 123 Main St. DeWitt, the map would recognize 123 Main St. Is really in DeWitt Township and autocorrect the city.	Y				
27.0	Mapping feature where system automatically corrects spelling of street name based on the city of the address. Example if 123 Peterson Rd. Is typed, but based on the city name there is no Peterson Rd (spelled that way), instead the system finds and inputs correct name of Petersen Rd.	Y				
28.0	System must have ability for contractor or MSP administrator to update/correct map information within 2 weeks of requested addition or change.	Y				
29.0	Mapping feature in system must have ability to show towing preferences based on location on the map. So, in this area, use tow vendor A, vs in this area uses tow vendor B, areas indicated on map.	Y				
30.0	System must have ability to support/serve the MSP, which act as law enforcement for the entire State of Michigan's 10 million residents, in both the Upper Peninsula and Lower	Y				

	Peninsula. Troopers are located throughout the State and MSP has 4 dispatch centers.					
31.0	Software must have the ability to display fire/EMS dispatch types to 2 centers daily, but not at other 2 on a daily basis. However, have ability for those 2 without fire/EMS displayed, to access those dispatch types if needed when acting in a backup capacity.	Y				
32.0	Software must have the ability to customize fields in the CAD window per center, so each center has ability to have customized response codes, etc. that correspond with individual centers.	Y				
33.0	Software must have a cloud-based solution hosted by the Contractor. FedRAMP certified, Microsoft Azure or AWS gov cloud are preferred platforms, but others may be acceptable with proper State of Michigan Security review.	Y				
34.0	All Contractor servers must reside in the continental United States. No servers that would have MSP data on it, may reside outside the continental United States.	Y				
35.0	System should have a test environment for testing new upgrades, troubleshooting other issues that may arise, and training new users.	Y				
36.0	System must have ability to clone an incident, or way to easily add other	Y				

	agencies to incident after it is already in CAD.					
37.0	System must have ability to allow specific individual user set settings to be recalled when different users sign on, so individuals don't have to set preferences daily.	Y				
38.0	System must have audible notifications with the ability to toggle them on or off for different events or all together.	Y				
39.0	System must have visual indicators on incidents to help define priority or incident type, with ability to toggle them on or off for different events or all together.	Y				
40.0	System must have MSP defined disposition codes.	Y				
41.0	System should have ability to type an incident type name not relying just on a drop-down list or knowing an incident type code.	Y				
42.0	System must have settings for the nature of call types with call priority.	Y				
43.0	System must have way to identify duplicate calls.	Y				
44.0	System must have ability to see complaint history and advisories.	Y				
45.0	System must have ability to pull up the history for a specific time period. Example: Trooper or supervisor would have ability to pull all calls that person took on their shift at the end of their	Y				

	shift, and could incorporate into their daily report.					
46.0	System must have ability to choose how pending calls show by priority, location, nature, etc.	Y				
47.0	System must have ability to schedule held calls into an active entry.	Y				
48.0	System must have ability to recommend responders based on GPS location of responders.	Y				
49.0	This CAD system would have ability to communicate with other CAD systems utilized by various first responders through the entire State of Michigan. (CAD to CAD) <i>Communication between different systems based on NENA/APCO Emergency Incident Data Document (EIDD) standard.</i>	Y				
50.0	Must have the ability to integrate with Automotive Vehicle Location (AVL) software to show Vehicle locations on the map.	Y				
51.0	System must have ability to choose how pending calls show by priority, location, nature, etc.	Y				
52.0	Must have the ability to integrate with ProQA (Priority Dispatch software).	Y				
53.0	Must have the ability to integrate with Rapid SOS software.	Y				



54.0	Must have the ability to integrate with Lexis Nexis, Record Management System.	Y				
55.0	Must have ability to integrate with the Law Enforcement Information Network (LEIN)	Y				
56.0	System must have ability to cut information from an alternative source (different computer) and paste information into CAD. So, we can cut something from our State of Michigan Computer and paste in CAD, likely on different computer.	Y				
57.0	Retention for CAD records needs to be at least 1 year. Must have ability to save specific reports if needed longer due to investigation, etc. Flexibility on the 1 year must also be there in case current retention schedule changes to shorter or longer timeframe.	Y				
58.0	System must have ability to do instant messaging within the CAD system to communicate with others using the CAD system.	Y				
59.0	RESERVED					
60.0	System should have a tiered, role-based access control to allow some users the ability to have write access to some things vs others.	Y				
61.0	Ability to link separate incident entries to one incident if it is related. If adding new incident of response type, automatically link to that incident. If	Y				

	discovered later that incident A is related to incident B, then combine them at that point. Could possibly be a parent incident with ability to set up sub incidents associated with it.					
62.0	<p>Contractor will provide in-person training events at different locations in the State of Michigan prior to go-live, to train users on the capabilities of the new CAD system. State of Michigan does not reimburse or pay for Contractor travel expenses.</p> <ul style="list-style-type: none"> <li>• Need several training sessions at various times of day/night at each location to accommodate all 3 shifts.</li> <li>• Mandatory training for Dispatchers, voluntary training for Troopers and Motor Carrier Officers.</li> <li>• Number of events and locations will be determined by MSP and contractor prior to go-live based on number and type of users in each district.</li> </ul>	Y				
63.0	Prior to go-live, Contractor will provide 2 Train the Trainer type classes for a deeper technical dive into the CAD system for MSP CAD administrators and MSP trainers to learn the complexities of the system.	Y				

64.0	Contractor must provide on-line training guides/videos for people unable to attend in person training sessions and future hires.	Y				
65.0	Contractor will continue to provide training when new updates come out or on a regular interval to ensure trainers and CAD techs know capabilities of system and any changes/updates that have been made.	Y				
66.0	System should have the ability to filter/limit the information shared. Example: restrict the LEIN information in an incident when shared with a non-Law Enforcement agency.	Y				
67.0	System must have ability to automate process' to reduce the amount of manual steps for the users to process items. Example of automated process would be to automate creating Fire Run Cards.	Y				
68.0	System must have automated process to send incident notes directly from CAD to responding agency or allowing responding agency access to obtain a copy of the CAD incident when the call closes.	Y				
69.0	System must have ability to do customizable/filterable reports based off various data fields found within CAD.	Y				
70.0	System must have ability to do some standards reports such as but not limited to: Incidednt type report to see	Y				

	how many incidents of that type there are; total volume report-filterable based on location, jurisdiction, center, etc.; and historical AVL reports.					
<b>OPTIONAL</b>						
1.0	Software must have ability to integrate or accept data from other 911 Next Generation source products available to dispatch centers. i.e. RapidSOS, Prepared 9-1-1 for examples.	Y				
2.0	API integration with MSP Contractor Lexis Nexis programs LEIN and e-ACIS. Ability for dispatcher to pull complaint number from e-ACIS and tie it to the CAD incident number. Or ideally, CAD incident number would be same as the e-ACIS complaint number.	Y				
3.0	System has a flexible refresh rate for the Automotive Vehicle Location (AVL) in the mapping portion of CAD.	Y				
4.0	Ability to click on an incident and have the option to call the officer associated with that incident. (Possible tie to phone system)					Y
5.0	Possible integration with in-car Cameras, Michigan Department of Transportation (MDOT) Cameras, and/or Body Worn Cameras. Giving the ability for dispatchers to check on safety	Y				

	of Trooper should they not respond to radio check ins.					
6.0	Possible integration with MS Teams so instant messaging in Teams could be done.					Y
7.0	For system to have ability to do some functions via keyboard commands or mouse commands. Some people like to use mouse, some command features, and others a mix of both.	Y				
8.0	System should have ability to resize your incident entry window to enlarge or reduce to the size the user at the time wants/needs.	Y				
9.0	Integration with the Michigan MPSCS 800 MHz radio system.	Y				

## SCHEDULE B - PRICING

Pricing includes all costs for the licensing, support, implementation, and training for the Solution for the duration of the initial 5-year contract term along with 5-1-year option periods.

**Table A - Subscription License Model**

Subscription Based - Product Name	Annual License Subscription Fee (SaaS Fees)	Annual Tiered Pricing	Annual Enterprise Licensing – Unlimited Number of Users
Tyler Enterprise Public Safety software and recurring fees (includes software subscription, AWS hosting, Tyler Managed Services, and maintenance on third-party software) Years 1-5	\$5,245,920.00		Unlimited
Year 6	\$1,362,816		
Year 7	\$1,430,957		
Year 8	\$1,502,505		
Year 9	\$1,577,630		
Year 10	\$1,656,511		

SaaS Fees are invoiced annually in advance commencing on the Effective Date, November 1, 2024, in accordance with the rates set forth in the table below.

The contract pricing for Support Fees is based on a firm fixed fee.

1. Implementation Fees. All costs associated with Implementation Services are

included below (e.g. configuration, customization, migration, integration, testing, etc.) (the “**Implementation Fees**”). All costs are firm fixed. Services are billed based on established milestones set forth in Section 24 of the Statement of Work.

2. Rate Card for Ancillary Professional Services.

Resource	On-Site Hourly Rate	Remote Hourly Rate
Project Management and Custom Development	\$160, plus per diem	\$160
Implementation and Services	\$145, plus per diem	\$145

Ancillary professional services (e.g. future enhancements configuration services)

3. Open Source or Third Party Products

Product	Price
Embedded Third-Party Software	Price included in SaaS Fees
Geo-File Maintenance Software (ArcGIS for Desktop Standard)	Removed from Pricing – State of Michigan will Procure

4. Hardware Pricing

Product	Price
Lantronix UDS-1100	Removed from Pricing – State of Michigan will Procure
Redundant VPN Appliance Bundle	Included at No Cost

5. Additional Pricing Terms

Quick payment terms: Not offered.

**Invoice Requirements**

All invoices submitted to the State must include: (a) date; (b) purchase order or delivery order; (c) quantity; (d) description of the Solution; (e) unit price; (f) shipping cost (if any); (g) Contractor-generated invoice number and (h) total price.

**Travel and Expenses**

The State does not pay for overtime or travel expenses.

SaaS and Implementation Fees Breakdown

Year	SaaS Fee	Implementation Fees
Year 1	\$600,000.00	\$760,030.00
Year 2	\$900,000.00	
Year 3	\$1,200,000.00	
Year 4	\$1,248,000.00	
Year 5	\$1,297,920.00	
<b>Five-Year Cost:</b>	<b>\$5,245,920.00</b>	<b>\$760,030.00</b>
Year 6	\$1,362,816.00	
Year 7	\$1,430,957.00	
Year 8	\$1,502,505.00	
Year 9	\$1,577,630.00	
Year 10	\$1,656,511.00	
<b>Ten-Year Cost:</b>	<b>\$12,776,339.00</b>	<b>\$760,030.00</b>

Annual SaaS Fees include Contractor's Enterprise Public-Safety, AWS GovCloud hosting and environment managed services.



ANNUAL/SAAS
<b>Platform</b> <ul style="list-style-type: none"> <li>• EPS Platform - Standard</li> <li>• EPS Platform - Mobility</li> </ul> <b>Computer Aided Dispatch</b> <ul style="list-style-type: none"> <li>• Enterprise CAD Combined LE/Fire/EMS</li> <li>• CAD NCIC Interface</li> <li>• Web CAD Monitor</li> <li>• CAD CFS (xml) Export Interface</li> <li>• CAD to CAD Interface</li> <li>• NG911 Interface (text to 911)</li> <li>• Unit Management</li> <li>• BOLOs</li> <li>• CAD AVL</li> <li>• CAD Auto Routing</li> <li>• Service Vehicle Rotation (Wrecker, Ambulance)</li> <li>• E-911 Interface</li> <li>• CAD Paging Interface</li> <li>• Pictometry Interface</li> <li>• Pre-Arrival Questionnaire Interface</li> <li>• CAD Data Mart / Includes 2 users</li> </ul> <b>Law Enforcement Records Management System</b> <ul style="list-style-type: none"> <li>• Public Safety Analytics (Performance Dashboard, Citizen Connect, Explorer, Analytics)</li> </ul> <b>Mobile</b> <ul style="list-style-type: none"> <li>• Enterprise Law Enforcement Mobile Server Software</li> <li>• Law Enforcement Mobile Site License</li> <li>• Fire/EMS Mobile Site License</li> </ul> <b>Other</b> <ul style="list-style-type: none"> <li>• Data Archive</li> <li>• Workstation License</li> <li>• Annual Enhanced Data Breach notification services are included in SaaS Fees</li> </ul>

**Services**

Description	Quantity	Total
Enterprise Public Safety		
Project Management	1	\$ 280,055
Standard System Assurance and Software Installation	2	\$ 18,560
Mobility Implementation	1	\$ 2,320
GIS Implementation	3	\$ 67,860
Decision Support Software Service	1	\$ 4,350
NCIC Installation	1	\$ 21,025
Combined or Fire/EMS CAD Configuration (3 or more PSAPs)	2	\$ 52,200
CAD Training (10 users ea.)	10	\$ 43,500
CAD Go-Live Support	2	\$ 43,500
Additional CAD Go-Live (per PSAP)	3	\$ 26,100
Web CAD Monitor Installation	1	\$ 1,160
CAD Paging Interface Installation	1	\$ 1,160
E-911 Interface Installation	1	\$ 1,160
NG911 Interface Installation	1	\$ 1,450
Pictometry Interface Installation	1	\$ 580
Pre-Arrival Questionnaire Interface Installation	3	\$ 3,480
CAD Export Interface Installation Fee	1	\$ 2,320
Law Enforcement and Fire Mobile Messaging Configuration	4	\$ 17,400
Law Enforcement and Fire Mobile Messaging Training (includes 10 trainers ea.)	3	\$ 26,100
Law Enforcement and Fire Mobile Messaging Go-Live	3	\$ 65,250
Public Safety Analytics Installation & Remote Training	1	\$ 4,500
Custom Interface to Lexis Nexis RMS (one-way)	1	\$ 14,400
Custom Interface to Motorola P25 Radio (two-way)	1	\$ 25,600
Data Archive Conversions		\$ 36,000
<b>TOTAL</b>		<b>\$ 760,030</b>

Below cost table is included for Contractor's internal accounting purposes only. These cost have no bearing on the fees to be paid by the State above.

COSTS		
	One-Time Fees	Recurring Fees
Software License Fees	\$ 0.00	\$ 0.00
SaaS Fees	\$ 0.00	\$ 1,250,011.00
Services	\$ 760,030.00	\$ 0.00
Third-Party Hardware, Software, Services	\$ 0.00	\$ 0.00
Estimated Travel Expenses	\$ 0.00	\$ 0.00
<b>Total</b>	<b>\$ 760,030.00</b>	<b>\$ 1,250,011.00</b>

## SCHEDULE C - INSURANCE REQUIREMENTS

---

1. **General Requirements.** Contractor, at its sole expense, must maintain the insurance coverage as specified herein for the duration of the Term. Minimum limits may be satisfied by any combination of primary liability, umbrella or excess liability, and self-insurance coverage. To the extent damages are covered by any required insurance, Contractor waives all rights against the State for such damages. Failure to maintain required insurance does not limit this waiver.
2. **Qualification of Insurers.** Except for self-insured coverage, all policies must be written by an insurer with an A.M. Best rating of A- VII or higher unless otherwise approved by DTMB Enterprise Risk Management.
3. **Primary and Non-Contributory Coverage.** All policies for which the State of Michigan is required to be named as an additional insured must be on a primary and non-contributory basis.
4. **Claims-Made Coverage.** If any required policies provide claims-made coverage, Contractor must:
  - a. Maintain coverage and provide evidence of coverage for at least 3 years after the later of the expiration or termination of the Contract or the completion of all its duties under the Contract;
  - b. Purchase extended reporting coverage for a minimum of 3 years after completion of work if coverage is cancelled or not renewed, and not replaced with another claims-made policy form with a retroactive date prior to the Effective Date of this Contract.
5. **Proof of Insurance.**
  - a. Insurance certificates showing evidence of coverage as required herein must be submitted to [DTMB-RiskManagement@michigan.gov](mailto:DTMB-RiskManagement@michigan.gov) within 10 days of the contract execution date.
  - b. Renewal insurance certificates must be provided on annual basis or as otherwise commensurate with the effective dates of coverage for any insurance required herein.
  - c. Insurance certificates must be in the form of a standard ACORD Insurance Certificate unless otherwise approved by DTMB Enterprise Risk Management.
  - d. All insurance certificates must clearly identify the Contract Number (e.g., notated under the Description of Operations on an ACORD form).
  - e. RESERVED.

- f. In the event any required coverage is cancelled or not renewed, Contractor must provide written notice to DTMB Enterprise Risk Management no later than 5 business days following such cancellation or nonrenewal.
6. **Subcontractors.** Contractor is responsible for ensuring its subcontractors carry and maintain insurance coverage.
7. **Limits of Coverage & Specific Endorsements.**

Required Limits	Additional Requirements
<b>Commercial General Liability Insurance</b>	
<b>Minimum Limits:</b> <b>\$1,000,000 Each Occurrence</b> <b>\$1,000,000 Personal &amp; Advertising Injury</b> <b>\$2,000,000 Products/Completed Operations</b> <b>\$2,000,000 General Aggregate</b>	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 20 10 12 19 and CG 20 37 12 19.
<b>Automobile Liability Insurance</b>	
<b>If a motor vehicle is used in relation to the Contractor's performance, the Contractor must have vehicle liability insurance on the motor vehicle for bodily injury and property damage as required by law.</b>	
<b>Workers' Compensation Insurance</b>	
<b>Minimum Limits:</b> <b>Coverage according to applicable laws governing work activities.</b>	Waiver of subrogation, except where waiver is prohibited by law.
<b>Employers Liability Insurance</b>	
<b>Minimum Limits:</b> <b>\$500,000 Each Accident</b> <b>\$500,000 Each Employee by Disease</b> <b>\$500,000 Aggregate Disease</b>	
<b>Privacy and Security Liability (Cyber Liability) and Professional Liability Insurance</b>	

Required Limits	Additional Requirements
<b>Minimum Limits:</b> <b>\$3,000,000</b>	Contractor must have their Cyber liability policy cover information security and privacy liability, privacy notification costs, regulatory defense and penalties, and website media content liability.

**Non-Waiver.** This Schedule C is not intended to and is not to 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.

# SCHEDULE D – SERVICE LEVEL AGREEMENT

---

## Agreement Overview

This SLA operates in conjunction with, and does not supersede or replace any part of, the Agreement. It outlines the information technology service levels that Contractor (“we”, “our”, or “Tyler”) will provide to the State (“you”, “your”, or “Client”) to ensure the availability of the application services that you have requested us to provide. All other support services are documented in the Support Call Process.

**II. Definitions.** Except as defined below, all defined terms have the meaning set forth in the Agreement.

*Actual Attainment:* The percentage of time the Tyler Software is available during a calendar quarter, calculated as follows:  $(\text{Service Availability} - \text{Downtime}) \div \text{Service Availability}$ .

*Client Error Incident:* Any service unavailability resulting from your applications, content or equipment, or the acts or omissions of any of your service users or your third-party providers over whom we exercise no control.

*Downtime:* Those minutes during Service Availability, as defined below, when all the Client’s users cannot launch, login, search or save primary data in the Tyler Software.

*Emergency Maintenance:* (1) maintenance that is required to patch a critical security vulnerability; (2) maintenance that is required to prevent an imminent outage of Service Availability; or (3) maintenance that is mutually agreed upon in writing by Tyler and the Client.

*Planned Downtime:* Downtime that occurs during a Standard or Emergency Maintenance window.

*"RPO" or "Recovery Point Objective"* means the maximum duration of time between the most recent recoverable copy of the State’s hosted Data and subsequent unavailability of Hosted Services.

*"RTO" or "Recovery Time Objective"* means the maximum period of time to fully restore the Hosted Services in the case of a disaster.

*Service Availability:* The total number of minutes in a calendar quarter that the Tyler Software is capable of receiving, processing, and responding to requests, excluding Planned Downtime, Client Error Incidents, denial of service attacks and Force Majeure. For clarity, in the event of a denial of service attack or Force Majeure event, as soon as the Services are capable of being recovered, such events will no longer be excluded from Service Availability.

*Standard Maintenance:* Routine maintenance to the Tyler Software and infrastructure. Standard Maintenance is limited to five (5) hours per week.

*Tyler Software:* The Software as defined in the Contract terms.

### III. Service Availability

#### a. Your Responsibilities

Whenever you experience Downtime, in order to be eligible for Client Relief, you must make a support call according to the procedures outlined in the Support Call Process. You will receive a support case number.

#### b. Our Responsibilities

When our support team receives a call from you that Downtime has occurred or is occurring, we will work with you to identify the cause of the Downtime (including whether it may be the result of Planned Downtime, a Client Error Incident, Denial of Service attack or Force Majeure). We will also work with you to resume normal operations.

#### c. Client Relief

Our targeted Attainment Goal is 100%. You may be entitled to credits as indicated in the Client Relief Schedule found below. Your relief credit is calculated as a percentage of the SaaS fees paid for the calendar quarter.

In the event Downtime results in relief credits, Tyler will provide a Software Service Availability report at the end of each applicable calendar quarter. 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 Attainment relative to the Attainment Goal; and (b) if Actual Attainment has failed in any respect to meet or exceed the Attainment Goal 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 Attainment Goal is fully met.

In order to receive relief credits, you must submit a request through one of the Support Channels listed in our Support Call Process within fifteen days (15) of the end of the applicable quarter. We will respond to your relief request within thirty (30) day(s) of receipt.

The total credits confirmed by us will be applied to the SaaS Fees for the next billing cycle. Issuing of such credit does not relieve us of our obligations under the Agreement to correct the problem which created the service interruption.

Client Relief Schedule	
Actual Attainment	Client Relief
99.99% - 99.90%	Remedial action will be taken
99.89% - 99.50%	2%
99.49% - 99.00%	4%

98.99% - 98.50%	6%
98.49% - 98.00%	8%
97.99% - 97.50%	10%
97.49% - 97.00%	12%
96.99% - 96.50%	14%
96.49% - 96.00%	16%
95.99% - 95.50%	18%
Below 95.50%	20%

#### **IV. Maintenance Notifications**

We perform Standard Maintenance during limited windows that are historically known to be reliably low-traffic times. If and when maintenance is predicted to occur during periods of higher traffic, we will provide a minimum of five (5) Business Days advance notice of those windows and will coordinate to the greatest extent possible with you.

Not all maintenance activities will cause application unavailability. However, if Tyler anticipates that activities during a Standard or Emergency Maintenance window may make the Tyler Software unavailable, we will provide a minimum of five (5) Business Days advance notice, as reasonably practicable that the Tyler Software will be unavailable during the maintenance window; however, the advance notice may be shorter in the event of Emergency Maintenance

#### **V. Additional Remedies for Service Level Failures**

In the event the State determines that Tyler is providing service levels that are repeatedly inconsistent with this Service Level Agreement, the State will escalate to Tyler executives in accordance with the Incident Escalation Process under the Support Call Process. In the event Tyler fails to engage with the State to create a mutually agreed upon action plan, the State may terminate for cause in accordance with the applicable termination provisions under the Agreement.

#### **VI. Disaster Recovery**

Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will maintain and operate a backup and disaster recovery plan, specific to the application production environment, to achieve a Recovery Point Objective (RPO) of 2 hours, and a Recovery Time Objective (RTO) of 8 hours (the "DR Plan"), and implement such DR Plan in the event of any disaster that renders the data centers unrecoverable. Contractor's current DR Plan has been provided to the State as of the Effective Date. Contractor will actively test, review and update the DR Plan on at least an annual basis using industry best practices as guidance. Contractor will provide the State with copies of all such updates to the Plan within thirty (30) days of its adoption by Contractor. All



updates to the DR Plan are subject to the requirements of this Section; and Contractor will provide the State with copies of all reports resulting from any testing of or pursuant to the DR Plan promptly after Contractor's receipt or preparation.

## Exhibit 1

### Support Call Process for Computer Aided Dispatch Software

#### Support Channels

Tyler Technologies, Inc. provides the following channels of software support for authorized users\*:

- (1) On-line submission (portal) – for less urgent and functionality-based questions, users may create support incidents through the Tyler Customer Portal available at the Tyler Technologies website. A built-in Answer Panel provides users with resolutions to most “how-to” and configuration-based questions through a simplified search interface with machine learning, potentially eliminating the need to submit the support case.
- (2) Email – for less urgent situations, users may submit emails directly to the software support group.
- (3) Telephone – for urgent or complex questions, users receive toll-free, telephone software support.

*\* Channel availability may be limited for certain applications.*

#### Support Resources

A number of additional resources are available to provide a comprehensive and complete support experience:

- (1) Tyler Website – [www.tylertech.com](http://www.tylertech.com) – for accessing client tools, documentation, and other information including support contact information.
- (2) Tyler Search -a knowledge based search engine that lets you search multiple sources simultaneously to find the answers you need, 24x7.
- (3) Tyler Community –provides a venue for all Tyler clients with current maintenance agreements to collaborate with one another, share best practices and resources, and access documentation.
- (4) Tyler University – online training courses on Tyler products.

#### Support Availability

Tyler Technologies support is available during the local business hours of 8 AM to 5 PM (Monday – Friday) across four US time zones (Pacific, Mountain, Central and Eastern) Tyler’s holiday schedule is outlined below. There will be no support coverage on these days for Priority Level 3 and 4 Defects. For clarity, Tyler provides 24 hours a day, 7 days a week, 365 days a year support for all Priority Level 1 Defects and for Priority Level 2 Defects that impact emergency operations.

New Year’s Day	Labor Day
Martin Luther King, Jr. Day	Thanksgiving Day
Memorial Day	Day after Thanksgiving

Independence Day	Christmas Day
------------------	---------------

## Incident Handling

### *Incident Tracking*

Every support incident is logged into Tyler’s Customer Relationship Management System and given a unique case number. This system tracks the history of each incident. The case number is used to track and reference open issues when clients contact support. Clients may track incidents, using the case number, through Tyler’s Customer Portal or by calling software support directly.

### *Incident Priority*

Each incident is assigned a priority level, which corresponds to the Client’s needs. Tyler and the Client will reasonably set the priority of the incident per the chart below. This chart is not intended to address every type of support incident, and certain “characteristics” may or may not apply depending on whether the Tyler software has been deployed on customer infrastructure or the Tyler cloud. The goal is to help guide the Client towards clearly understanding and communicating the importance of the issue and to describe generally expected response and resolution targets in the production environment only.

References to a “confirmed support incident” mean that Tyler and the Client have successfully validated the reported Defect/support incident.

Priority Level	Characteristics of Support Incident	Resolution Targets
1 Critical	Support incident that causes (a) complete application failure or application unavailability; (b) application failure or unavailability in one or more of the client’s remote location; or (c) systemic loss of multiple essential system functions.	Tyler shall provide an initial response to Priority Level 1 incidents within one (1) hour of receipt of the incident. Once the incident has been confirmed, Tyler shall use commercially reasonable efforts to resolve such support incidents or provide a circumvention procedure within one (1) day.

Priority Level	Characteristics of Support Incident	Resolution Targets
2 High	Support incident that causes (a) repeated, consistent failure of essential functionality affecting more than one user or (b) loss or corruption of data.	Except for Priority Level 2 incidents impacting emergency operations which will be treated as Priority Level 1 for Resolution Targets, Tyler shall provide an initial response to Priority Level 2 incidents within four (4) business hours of receipt of the incident. Once the incident has been confirmed, Tyler shall use commercially reasonable efforts to resolve such support incidents or provide a circumvention procedure within ten (10) business days.
3 Medium	Priority Level 1 incident with an existing circumvention procedure, or a Priority Level 2 incident that affects only one user or for which there is an existing circumvention procedure.	Tyler shall provide an initial response to Priority Level 3 incidents within one (1) business day of receipt of the incident. Once the incident has been confirmed, Tyler shall use commercially reasonable efforts to resolve such support incidents without the need for a circumvention procedure with the next published maintenance update or service pack, which shall occur at least quarterly.
4 Non-critical	Support incident that causes failure of non-essential functionality or a cosmetic or other issue that does not qualify as any other Priority Level.	Tyler shall provide an initial response to Priority Level 4 incidents within two (2) business days of receipt of the incident. Once the incident has been confirmed, Tyler shall use commercially reasonable efforts to resolve such support incidents, as well as cosmetic issues, with a future version release.

#### *Incident Escalation*

If Tyler is unable to resolve any priority level 1 or 2 defect as listed above or the priority of an issue has elevated since initiation, Tyler will escalate the incident to the appropriate resource, as outlined by each product support team. The corresponding resource will meet with you and any Tyler staff to establish a mutually agreeable plan for addressing the defect.

#### *Remote Support Tool*

Some support calls may require further analysis of the Client's database, processes or setup to diagnose a problem or to assist with a question. Tyler will, at its discretion, use an industry-standard remote

support tool. Tyler's support team must have the ability to quickly connect to the Client's system and view the site's setup, diagnose problems, or assist with screen navigation. More information about the remote support tool Tyler uses is available upon request.

## SCHEDULE D – ATTACHMENT 1 – CONTACT LIST

---

Level 1	Support Representative – contact will vary based on issue
Level 2	Senior Client Success Account Manager – Angi Ostrom, (248) 269-1000
Level 3	Director of Support Services – Debra Viselli, (248) 269-1000, ext. 1396
Level 4	Vice President of Client Success – Paul Case, (248) 269-1000, ext. 1438
Level 5	President – Andrew B. Hittle, (248) 269-1000

## **SCHEDULE E – DATA SECURITY REQUIREMENTS**

---

**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 **Schedule** 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.

**“FedRAMP”** means the Federal Risk and Authorization Management 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.

**“FISMA”** means The Federal Information Security Modernization Act of 2014 (Pub.L. No. 113-283 (Dec. 18, 2014.)).

**“Hosting Provider”** means any Permitted Subcontractor that is providing any or all of the Hosted Services under this Contract.

**“NIST”** means the National Institute of Standards and Technology.

**“PCI”** means the Payment Card Industry.

**“PSP”** or **“PSPs”** means the State’s IT Policies, Standards and Procedures.

**“SSAE”** means Statement on Standards for Attestation Engagements.

**“Security Accreditation Process”** has the meaning set forth in **Section 6** of this Schedule

**2. Security Officer.** Contractor will appoint a Contractor employee to respond to the State’s inquiries regarding the security of the Hosted Services who has sufficient knowledge of the security of the Hosted Services and the authority to act on behalf of Contractor in matters pertaining thereto (**“Contractor Security Officer”**).

**3. Contractor Responsibilities.** 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 any State Data in Contractor's or its subcontractor's possession; and
- (e) ensure that all Contractor Personnel comply with the foregoing.

The State has established Information Technology (IT) PSPs to protect IT resources under the authority outlined in the overarching State 1305.00 Enterprise IT Policy. In no case will the safeguards of Contractor's data privacy and information security program be less stringent than the safeguards used by the State or appropriate industry standards, and Contractor must at all times comply with all applicable public and non-public State IT policies and standards, as of the Effective Date, and thereafter as mutually agreed upon in writing, of which the publicly available ones are at <https://www.michigan.gov/dtmb/policies/it-policies>.

This responsibility also extends to all service providers and subcontractors with access to State Data or an ability to impact the contracted solution. Contractor responsibilities are determined from the PSPs based on the services being provided to the State, the type of IT solution, and the applicable laws and regulations.

**4. Acceptable Use Standard.** To the extent that Contractor has access to the State's IT environment, Contractor must comply with the State's Acceptable Use Standard, see <https://www.michigan.gov/dtmb/-/media/Project/Websites/dtmb/Law-and-Policies/IT-Policy/13400013002-Acceptable-Use-of-Information-Technology-Standard.pdf>. All Contractor Personnel will be required, in writing, to agree to the State's Acceptable Use Standard before accessing State systems or Data. The State reserves the right to terminate Contractor's and/or subcontractor(s) or any Contractor Personnel's access to State systems if the State determines a violation has occurred.

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

5.1 If Hosted Services are provided by a Hosting Provider, ensure each Hosting Provider maintains FedRAMP authorization for all Hosted Services environments throughout the Term, and in the event a Hosting Provider is unable to maintain FedRAMP authorization, the State, at its sole discretion, may either a) require the Contractor to move the Software and State Data to an alternative Hosting Provider



selected and approved by the State at Contractor's sole cost and expense without any increase in Fees, or b) immediately terminate this Contract for cause.

5.2 for Hosted Services provided by the Contractor, maintain either a FedRAMP authorization or an annual SSAE 18 SOC 2 Type II audit based on State required NIST Special Publication 800-53 MOD Controls using identified controls and minimum values as established in applicable State PSPs.

5.3 ensure that the Software and State Data is securely stored, hosted, supported, administered, accessed, developed and backed up in the continental United States, and the data center(s) in which State Data resides minimally meets Uptime Institute Tier 3 standards (<https://www.uptimeinstitute.com/>), or its equivalent;-

5.4 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 Data that complies with industry standards as well as the applicable requirements of the State's data security policies as set forth in this Contract, and applicable requirements of FISMA and NIST Special Publication 800-53 MOD Controls using identified controls and minimum values as established in applicable State PSPs;

5.5 Throughout the Term, Contractor must not provide Hardware or Services from the list of excluded parties in the [System for Award Management \(SAM\)](#) for entities excluded from receiving federal government awards for "covered telecommunications equipment or services.

5.6 provide technical and organizational safeguards against accidental, unlawful or unauthorized access to or use, destruction, loss, alteration, disclosure, encryption, transfer, commingling or processing of such information that ensure a level of security appropriate to the risks presented by the processing of State Data and the nature of such State Data, consistent with best industry practice and applicable standards (including, but not limited to, compliance with FISMA, NIST, CMS, IRS, FBI, SSA, HIPAA, FERPA and PCI requirements as applicable);

5.7 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 "malicious actors" and others who may seek, without authorization, to destroy, disrupt,

damage, encrypt, modify, copy, access or otherwise use Hosted Services 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) State Data 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 Data;

5.8 ensure that State Data is encrypted in transit and at rest using FIPS validated AES encryption modules and a key size of 128 bits or higher;

5.9 ensure the Hosted Services support the State's Active Directory using secure LDAP (Lightweight Directory Access Protocol) or comparable State approved mechanisms;

5.10 ensure the Hosted Services implements NIST compliant multi-factor authentication for privileged/administrative and other identified access.

5.11 Contractor must permanently sanitize or destroy the State's information, including State Data, from all media both digital and nondigital including backups using National Security Agency ("NSA") and/or National Institute of Standards and Technology ("NIST") (NIST Guide for Media Sanitization 800-88) data sanitization methods or as otherwise instructed by the State. Contractor must sanitize information system media, both digital and non-digital, prior to disposal, release out of its control, or release for reuse as specified above.

**6. Security Accreditation Process.** Throughout the Term, Contractor will assist the State, at no additional cost, with its **Security Accreditation Process**, which includes the development, completion and on-going maintenance of a system security plan (SSP) using the State's automated governance, risk and compliance (GRC) platform, which requires Contractor to submit evidence, upon request from the State, in order to validate Contractor's security controls within two weeks of the State's request. On an annual basis, or as otherwise required by the State such as for significant changes, re-assessment of the system's controls will be required to receive and maintain authority to operate (ATO). All identified risks from the SSP will be remediated through a Plan of Action and Milestones (POAM) process with remediation time frames and required evidence based on the risk level of the identified risk. For all findings associated with the Contractor's solution, at no additional cost, Contractor will be required to create or assist with the creation of State approved POAMs, perform related remediation

activities, and provide evidence of compliance. The State will make any decisions on acceptable risk, Contractor may request risk acceptance, supported by compensating controls, however only the State may formally accept risk. Failure to comply with this section will be deemed a material breach of the Contract.

**7. Unauthorized Access.** Contractor may not access, and must not permit any access to State systems, in whole or in part, whether through the Hosted Services 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. All State-authorized connectivity or attempted connectivity to State systems shall be only through an industry standard secure tool called BeyondTrust, formerly Bomgar. Such connectivity shall be attended access only, approved in advance by the State.

## **8. Security Audits.**

8.1 During the Term, Contractor will maintain complete and accurate records of its data protection practices, IT security controls, and the security logs relating to State Data, including but not limited to any backup, disaster recovery or other policies, practices or procedures relating to the State Data and any other information relevant to its compliance with this Contract.

8.2 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. 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. If the State chooses to perform an on-site audit, Contractor will make available appropriate personnel, as well as all such records and materials that are directly relevant to this Contract, during normal business hours. Such records and materials will be made available for inspection and audit by the State or an independent data security expert that is reasonably acceptable to Contractor, provided that the State: (i) works with Contractor to select a mutually agreeable date and time for any such audit; (ii) undertakes such audit no more than once per calendar year, except for good cause shown; (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; and (iv) conducts such audit in a

manner that protects the confidentiality, integrity, availability and security of Contractor's systems and the data of Contractor's other customers. The State may, but is not obligated to, perform the foregoing security audits.

8.3 During the Term, Contractor will, when requested by the State, provide a copy of Contractor's and Hosting Provider's SOC 2 Type 2 report(s) to the State within two weeks of the State's request. The SSAE audit reports will be recognized as Contractor's Confidential Information.

8.4 Contractor must implement any required safeguards as identified by applicable law or by any audit of Contractor's data privacy and information security program.

8.5 The State reserves the right, at its sole election, to terminate this Contract or a Statement of Work without limitation and without liability if the State determines that Contractor fails or has failed to meet its obligations under this **Section 8.**

**9. Application Scanning.** During the Term, Contractor must, at its sole cost and expense, scan all Contractor provided applications, and must analyze, remediate and validate all vulnerabilities identified by the scans as required by Contractor's Vulnerability Remediation Timeframe (VRT) documentation, attached as Attachment 2 to this Schedule E. As of the effective date of this contract, Contractor acknowledges that its VRT complies with any applicable laws, including the FBI CJIS Security Policy Version 5.9.4. Any updates to Contractor's VRT must be mutually agreed to in writing by the parties, except for those updates that are required by law or future versions of the FBI CJIS Security Policy. For any updates required by law or the FBI CJIS Security Policy, Contractor will provide notice to the State within 10 days of making such change with a copy of the revised VRT.

Contractor's application scanning and remediation must include each of the following types of scans and activities:

9.1 Dynamic Application Security Testing (DAST) – Authenticated interactive scanning of application for vulnerabilities, analysis, remediation, and validation (may include Interactive Application Security Testing (IAST)).

(a) Contractor must dynamically scan a deployed version of the Software using a PCI approved application scanning tool and remediate any findings. These scans and assessments i) must be completed quarterly and for each major

release, and provide a scan summary which includes number of vulnerabilities by severity and monthly age ; and ii) scans must be completed in a non-production environment with verifiable matching source code and supporting infrastructure configurations or the actual production environment.

#### 9.2 Static Application Security Testing (SAST) - Scanning source code for vulnerabilities, analysis, remediation, and validation.

(a) For Contractor provided applications, Contractor, at its sole expense, must provide resources to complete static application source code scanning, including the analysis, remediation and validation of vulnerabilities identified by application source code scans. These scans must be completed for all source code initially, for all updated source code, and for all source code for each major release, and Contractor must provide to the State a scan summary which includes number of vulnerabilities by severity and monthly age.

#### 9.3 Software Composition Analysis (SCA) – Third Party and/or Open Source Scanning for vulnerabilities, analysis, remediation, and validation.

(a) For Software that includes third party and open source software, all included third party and open source software must be documented and the source supplier must be monitored by the Contractor for notification of identified vulnerabilities and remediation. SCA scans may be included as part of SAST and DAST scanning or employ the use of an SCA tool to meet the scanning requirements. These scans must be completed for all third party and open source software initially, for all updated third party and open source software, and for all third party and open source software in each major release, and Contractor must provide to the State a scan summary which includes number of vulnerabilities by severity and monthly age.

#### 9.4 In addition, application scanning and remediation may include the following types of scans and activities if required by regulatory or industry requirements, data classification or otherwise identified by the State.

(a) If provided as part of the solution, all native mobile application software must meet these scanning requirements including any interaction with an application programming interface (API).

(b) Penetration Testing – Simulated attack on the application and infrastructure to identify security weaknesses.

## **10. Infrastructure Scanning.**

10.1 For Hosted Services, Contractor must ensure the infrastructure and applications are scanned using an approved scanning tool (Qualys, Tenable, or other PCI Approved Vulnerability Scanning Tool) at least monthly and provide a scanned summary which includes number of vulnerabilities by severity and monthly age. Contractor will ensure the remediation of issues identified in the scan according to the remediation time requirements documented in Contractor's Vulnerability Remediation Timeframe documentation, attachment 2 of Schedule E.

## **11. Nonexclusive Remedy for Security Breach.**

11.1 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.

# **SCHEDULE E, ATTACHMENT 1 – CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)**

---

## **FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM**

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A- 130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

### **1.00 Definitions**

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

### **2.00 Responsibilities of the Contracting Government Agency.**

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

### 3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

### 4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

### 5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

### 6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road



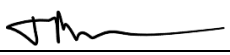
Clarksburg, West Virginia 26306

**FEDERAL BUREAU OF INVESTIGATION CRIMINAL  
JUSTICE INFORMATION SERVICES SECURITY  
ADDENDUM**

**CERTIFICATION**

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Tom Miller, Sales Dir. 

8/15/2023

Printed Name/Signature of Contractor Employee

Date

Andrew B. Hittle, President 

8/15/2023

Printed Name/Signature of Contractor Representative

Date

## SCHEDULE E, Attachment 2 – Contractor’s Vulnerability Remediation Timeframe (VRT)

Tyler Enterprise Public Safety (EPS) understands the importance of maintaining stringent security protocols and timely remediation of vulnerabilities in our software products. Since potential vulnerabilities are unique to each environment Tyler will start providing quarterly vulnerability reports the first month after go-live. Below is an outline of our commitment to addressing cloud application vulnerabilities to ensure the security and reliability of our applications. Tyler commits to the following remediation schedule:

Tyler EPS - Cloud Application Remediation Timeframe (in days)				
CVSS	Critical (9.0-10.0)	High (7.0-8.9)	Medium (4.0-6.9)	Low (0-3.9)
Action Plan	7	15	30	90
Resolution Time	30	60	90	180

When a critical vulnerability is released that affects the public facing Cisco VPN devices, Tyler engages our vendor immediately to determine if our configuration is in scope. In adherence with CJS guidelines and with written confirmation from our vendor that we are impacted by the critical vulnerability, Tyler commits to the following remediation schedule:

Tyler/Cisco - Public Facing Devices (VPNs) Remediation Timeframe (in days)				
CVSS	Critical (9.0-10.0)	High (7.0-8.9)	Medium (4.0-6.9)	Low (0-3.9)
Action Plan	7	15	30	30
Resolution Time	15	30	60	90

Tyler recommends that customers deploy the hardware VPN solution securely behind their edge firewall. A common deployment would include terminating both the trusted and untrusted interfaces into a secure DMZ. This allows the customer to apply additional security measures enabling them to secure all inbound and outbound communication. We will provide all source and destination IP and protocol information during deployment. In addition, Tyler uses a hardened configuration on the devices, enabling only the features required to manage the device and terminate VTI site to site VPN connectivity. All WebVPN and AnyConnect services are disabled. Management is secured by Tyler provided sources hosts only.

Tyler reserves the right to review each vulnerability individually and assess the critical nature and required response. In addition to patching, Tyler performs software updates that include security updates as part of our regular maintenance schedule and feature roll- ups to stay current with the software and firmware. These updates would be performed at our discretion outside of a

vulnerability release timetable.

The Tyler EPS cloud deployment also utilizes two public facing services from AWS, a network load balancer and an application load balancer. The following language was provided by an AWS Security Champion and is the AWS' official policy. As part of the FedRAMP authorization process, we must comply with RA-5d controls. Cloud Service

Providers (CSPs) must mitigate all discovered high-risk vulnerabilities within 30 days, mitigate moderate vulnerability risks in 90 days, and mitigate low vulnerability risks in 180 days. CSPs must send their Reviewer updated artifacts every 30 days to show evidence that outstanding high-risk vulnerabilities have been mitigated. AWS commits to the following remediation schedule:

AWS - Public Facing Devices (NLB/ALB) Remediation Timeframe (in days)				
CVSS	Critical (9.0-10.0)	High (7.0-8.9)	Medium (4.0-6.9)	Low (0-3.9)
Action Plan	7	15	30	30
Resolution Time	15 / Immediately*	30	90	180

At the government's discretion, FedRAMP or individual Agency Authorizing Official may direct the Cloud Service Provider (CSP) to treat certain critical vulnerabilities as incidents, such as "zero day" vulnerabilities (e.g., Heartbleed). \*CSPs must take immediate action to fully resolve the vulnerability if possible, or at least implement mitigating factors. The FedRAMP program management office may request immediate reporting on these items. FedRAMP may request immediate reporting on these critical vulnerabilities, both for Joint Authorization Board provisional authorization to operate and FedRAMP Agency authorization to operate systems. The CSP must continue to track critical vulnerabilities in the system's POA&M even when they are providing special reporting to FedRAMP.

## **SCHEDULE F – DISASTER RECOVERY PLAN**

**Schedule redacted for security reason**