STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget
525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **4**
to
Contract Number **180000000986**

CONTRACTOR	DELOITTE & TOUCHE LLP
	300 Renaissance Center
	Detroit, MI 48243
	Mark Ford
	313-394-5313
	mford@deloitte.com
	CV0002117

STATE	Program Manager	Jose Semidei	DTMB
		517-241-2661	
		Semideij@Michigan.gov	
	Contract Administrator	Jordan Sherlock	DTMB
		(517) 243-5556	
		SherlockJ@michigan.gov	

CONTRACT SUMMARY

APPSCAN REMEDIATION AND VALIDATION

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
July 30, 2018	December 31, 2018	4 - 1 Year	December 31, 2021

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-Card	☐ PRC	☐ Other	☒ Yes	☐ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$2,941,920.00	$546,000	$3,487,920.00

DESCRIPTION

Effective 3/30/2021, this Contract is incorporating the attached Statement of Work (SOW) for Michigan Cyber Security (MCS)'s DevSecOps efforts. In addition, this contract is increased by $546,000 to fund this engagement.

All other terms, conditions, specifications and pricing remain the same. Per contractor and agency agreement, DTMB Procurement approval, and State Administrative Board approval March 30th, 2021.

SCHEDULE A
STATEMENT OF WORK

1. Background and Scope

a. The Department of Technology, Management and Budget (DTMB) is executing this Statement of Work (SOW) under the AppScan Remediation and Validation Contract (#171-180000000986) ("Contract") to assist DTMB with establishing a program to help improve the security and the Application Lifecycle Management through the expansion of DevSecOps methodologies and provide the capability for DTMB to rapidly deploy application changes as needed to address delay in finding security issues as security scanning happens right before production deployment, manual setup of infrastructure and manual deployment of application releases.

b. The State of Michigan Department of Technology, Management and Budget (DTMB) has completed an assessment and pilot as detailed in Change Notice 2 of Contract (#171-180000000986)

c. To realize the potential benefits obtained in the pilot at scale, expansion of the DevSecOps capabilities is required across the State's application portfolio.

d. As part of this effort, DTMB has conducted agency wide Agile/DevSecOps assessments for selecting applications for onboarding. Contractor will assist in this effort, as required.

e. Contractor will execute the onboarding process for selected applications over a fixed 5-month duration as described in Section 4. DTMB will be responsible for identifying applications as detailed in Section 4. Onboarding effort will involve mix of coaching and implementation for applications selected based on assessment.

f. DTMB may elect to onboard additional applications beyond the fixed 5-month time as noted in the fee schedule in Schedule B, Table 4. Should the State decide to extend as noted in this section, the State shall provide the Contractor with a 30-day notice prior to the scheduled Sprint 4 end date indicating "intent to continue". The onboarding process, assumptions and requirements noted in this SOW apply to subsequent sprints. Pricing for additional sprints is included in Schedule B, Pricing

g. For the fixed capacity planned in each Sprint, DTMB will prioritize activities for the Contractor, within the noted capacity percentages. The prioritization will happen through items entered into the DevOps Azure tool which the Contractor will implement in Sprint 0. Items for prioritization will be within the scope of the activities listed below:

i. <u>**Governance and Adoption**</u>

- ***Outreach –*** Using the agency Agile/DevSecOps assessment results as a guide, assist the State in taking the mature practices/processes already in use by higher scoring teams (optimized or leading) for the 13 competencies evaluated, and sharing the benefits and results of these practices/processes to other agencies/teams.
- ***Containerization Architecture Assistance –*** Per the agency Agile/DevSecOps assessment results, some teams assessed have set-up containers that are productive for DevSecOps activities. Assist the State in creating an onboarding

mechanism to assist agencies in setting up containers modeled off the teams that have done it.

- ***Tool Analysis –*** Per the agency DevSecOps assessment results, a variety of different tool sets that offer the same functionality are being used across the 13 competencies. Assist the State in identifying core tools to be used in a catalog for agency adoption. Tools identified will be documented and include the value proposition they provide to the State for State use.
- ***Azure DevOps training –*** Contractor will work with DTMB to develop ADO Dojo material for rolling out to agencies. DTMB will be responsible for identifying resources and managing the schedules for the trainings.
- ***DevSecOps training inclusion –*** The State has several recorded training Dojos' that the Contractor previously provided to the State as deliverables per past change notices on this contract. Contractor will assist the State in rolling these trainings into the State's broader enterprise learning management system. If additional training resources on the general concept of DevSecOps are found that are available to the State already, include those trainings in inclusion to the enterprise system as well.
- ***Metrics and KPI's -*** Building upon the metrics and KPI deliverables provided to the State as part of previous change notices on this contract, assist the State in creating an enterprise-wide standard mechanism for measuring efficiencies gained as they adopt DevSecOps specific to the 13 competencies.
- ***Sustainability –*** Assist the State in developing a sustainability plan that includes considerations related to metrics, KPI's and the frequency of evaluating those measures, to bring all agencies/project teams to level 4 (optimized) or level 5 (leading) status.

ii. <u>Implementation/Engineering</u>

- ***Entry criteria –*** The State/DTMB will provide a list of applications / enhancements that are (or will be) in an active status beginning March 1st for DevSecOps transformation. Contractor will identify specific "needs" areas across the 13 competencies that, based on the agency Agile/DevSecOps assessment results, are best suited for improvement across the enterprise.
- ***Onboarding –*** Contractor will execute the onboarding process for selected applications based on the list prioritized by the State (see bullet above) over a fixed 5-month duration. The selected applications will be onboarded using templates as described in Section 4.
- ***Engagement activities –*** Contractor will develop a dashboard strategy based on KPIs to demonstrate benefits realized. Contractor will do the analysis of selected applications to develop onboarding patterns and will design and test onboarding templates. Contractor will also provide Value Stream Mapping (pre- and post-onboarding) to measure success.
- ***Outcome measures –*** The applications onboarded, training via Dojos conducted, and coaching provided to the teams will be measured via Value Stream Mapping (VSM). Knowledge transfer and transition of new DevSecOps capabilities to DTMB Application Teams.

DTMB is responsible for identifying and prioritizing applications through assessment to be placed in the backlog with prior to start of Sprint 0. DTMB shall notify the Contractor via email with the identified applications, and the Contractor shall email back receipt of the email noting the applications are approved applications.

The engagement will start March 8th, 2021 with 5 planned sprint cycles and each sprint cycle will be 4 weeks long. The project is anticipated to end on July 23rd, 2021, unless DTMB elects to add additional applications per Section 1(e).

DTMB acknowledges that the scope of Contractor's project activities does not include handling of any protected health information (PHI), personally identifiable information (PII), and/or payment card information (PCI) within the existing systems or applications in the scope of this project.

2. Project Management

Enterprise Project Management Office (EPMO) SUITE Process

Contractor will follow the EPMO standard State Unified Information Technology Environment (SUITE) process or obtain prior State approval to implement modifications. SUITE is a project management methodology used by the State of Michigan.

3. Project Charter and Project Plan

The State and Contractor will jointly draft a project charter. Contractor will create a project plan with input from the State. The project plan will be reviewed by State on a regular basis including bi-weekly Steering Committee meetings. The State Project Manager will maintain the project plan and review with the State and Contractor in the weekly status meetings identified in Section 11 (a) – Meetings.

a. A **Project Backlog** will include a list of prioritized items that DTMB would like to accomplish as part of the DevSecOps transformation. This project backlog will be maintained all through the life of the project based on DTMB priorities and will feed in scoping individual Sprint plans. The contractor will be responsible for providing DTMB with storypoints/t-shirt sizing for backlog items identified so they can use that for planning the sprint scope and priorities.

b. A **Sprint Plan** will be used to finalize scope in each sprint backlog, roles & responsibilities and timelines. The sprint backlog will be planned and prioritized by DTMB from Section 1 (g) based on agencies needs and availability.

4. Approach to DevSecOps Adoption

To rapidly onboard applications for the State to transition to a DevSecOps model, the following steps will be performed.

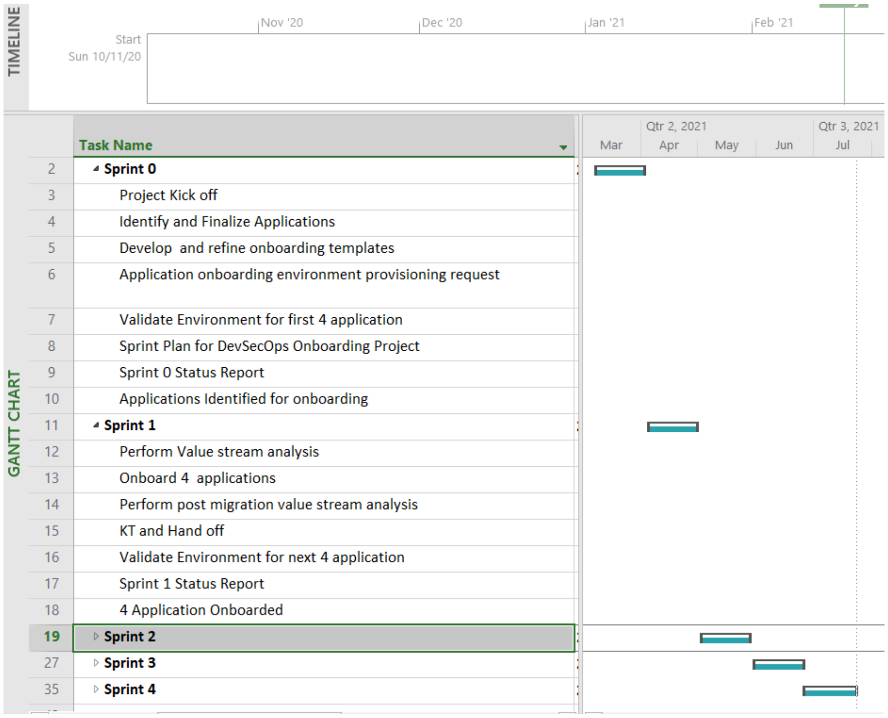
Sprint and Timing (Sprint Duration: 4 weeks)	Activities and Deliverables
Sprint 0	Contractor will start the project with a project kickoff meeting to align with State leadership and set direction for overall project. The kickoff meeting will happen Week 1 of the project. Contractor will finalize teaming structure and engage with subset of identified teams through a combination of implementation, training Dojos, and coaching.

Sprint and Timing (Sprint Duration: 4 weeks)	Activities and Deliverables
	Entry Criteria: • DTMB provides applications for DevSecOps transformation • DTMB confirms the which of the 13 capabilities are applicable for the applications identified (for State prioritization purposes, less capacity/storypoints will be needed for the 3 capabilities covered in the previous Proof of Concept – Version Control, Shift Left on Security, and Release Management) • DTMB identifies the backlog items aligned with Section 1(g) Activities (subject to backlog prioritization): ▪ Contractor will develop a DevSecOps project Sprint backlog in Azure DevOps tool. ▪ Contractor will develop dashboard strategy based on KPIs to demonstrate benefits realized. from onboarding application to DevSecOps model ▪ Contractor will do the analysis of selected applications in the backlog que to develop onboarding patterns ▪ Contractor will develop t-shirt sizing for the backlog items identified by DTMB ▪ DTMB will prioritize the backlog items ▪ The Contractor will develop a Sprint 1 plan with the prioritized backlog items that aligns to the fixed capacity available ▪ Contractor will design and test onboarding templates ▪ Contractor will do Value Stream Mapping (pre- and post-onboarding) for Sprint 1 prioritized applications ▪ Contractor will plan for Dojo trainings Deliverables: • Sprint Plan • Sprint 0 Status Report • Sprint Backlog in Azure DevOps Exit Criteria: • Sprint backlog, training Dojos material • Efficiencies planned through Value Stream Mapping (VSM) • DTMB Sprint review and signoff
Task/Sprint 1-4	Contractor will continue to provide Governance and Implementation Engineering support (onboard applications, provide coaching and run training Dojos) as prioritized by DTMB per the Sprint plan. Entry Criteria (prior to start of Sprint 1): • DTMB provides applications for DevSecOps transformation • DTMB confirms the 13 capabilities applicable for the applications identified (focus will be for the 3 capabilities – Version Control, Shift Left on Security, and Release Management) • DTMB identifies the backlog items aligned with Section 1(g) Activities (subject to backlog prioritization): • The Contractor will develop a Sprint plan for each sprint, 1-4, with the prioritized backlog items with the capacity available

Sprint and Timing (Sprint Duration: 4 weeks)	Activities and Deliverables
	• Contractor will develop checklist for onboarding applications • Contractor will design and test onboarding templates • Contractor will do Value Stream Mapping (pre- and post-onboarding) for Sprint 1-4 prioritized applications • Contractor will deliver for Dojo trainings for the modules to the application teams delivered • State will review and approve the Sprint n+1 plan specific to the active sprint Deliverables: • Project Backlog • Sprint 1 Status Report (end of Sprint 1 completion) • Sprint 2 Status Report (end of Sprint 2 completion) • Sprint 3 Status Report (end of Sprint 3 completion) • Sprint 4 Status Report (end of Sprint 4 completion) • DevSecOps Onboard Summary Report (within 2 weeks of completion of last Sprint) Exit Criteria (end of each sprint): • Application onboarded with the defined DevSecOps capabilities • Efficiencies measured through Value Stream Mapping (VSM) • Knowledge transfer and transition of new DevSecOps capabilities to DTMB Application Teams • DTMB Sprint review and signoff • DTMB review and signoff on the final DevSecOps Onboard Summary Report (applicable for only Sprint 4)

Table 1: Sprint Plan that outlines the Sprint cycles, activities and deliverables

The tasks described above will take place according to the following timeline. Activity and deliverable dates will be detailed in the Sprint Plan deliverable due to the State by the end of project week 3. Task durations are representative and may vary from the chart below depending on the application being onboarded.



	Task Name
2	◢ **Sprint 0**
3	Project Kick off
4	Identify and Finalize Applications
5	Develop and refine onboarding templates
6	Application onboarding environment provisioning request
7	Validate Environment for first 4 application
8	Sprint Plan for DevSecOps Onboarding Project
9	Sprint 0 Status Report
10	Applications Identified for onboarding
11	◢ **Sprint 1**
12	Perform Value stream analysis
13	Onboard 4 applications
14	Perform post migration value stream analysis
15	KT and Hand off
16	Validate Environment for next 4 application
17	Sprint 1 Status Report
18	4 Application Onboarded
19	▷ **Sprint 2**
27	▷ **Sprint 3**
35	▷ **Sprint 4**

Figure 1: Sprint Plan with key activities and dates

5. Acceptance Criteria

All documents will be work products delivered by the combined Contractor and State team. Acceptance timeframes for supporting work products will be strictly enforced in accordance with the table below.

Work Product	Initial Review (From the day of submission)	Deloitte Response (From the day of response)	Final Review (From the day of re-submission)
Sprint Plan for DevSecOps Project	5 business days	2 business day	3 business days
Sprint Status Report	5 business days	2 business day	3 business days
DevSecOps Onboard Summary Report	5 business days	2 business day	3 business days

6. Staffing

a. **Work Hours** Contractor will primarily work during State business hours Monday – Friday from 8:00am to 5:00pm Eastern time but may also work outside of these hours and on weekends.

b. **Work Location** Contractor will work remotely, and all work will be performed within the United States. The State will provide office space for Contractor's team if onsite work is required during the project.

7. State Project Contacts

Role	Name	Title	Responsibility
Executive Sponsor	Jim Hogan	DTMB General Manager	The Executive Sponsor (a) administers the terms of this SOW, and (b) serves as the primary contact with regards to the advisement of the execution of work contained in this SOW who will have the authority to act on behalf of the State.
Co-Sponsor	Cindy Peruchietti	Deputy Director – Agency Services	Active participation in the Project Steering Committee
Co-Sponsor	Eric Swanson	Deputy Director – Center for Shared Solutions	Active participation in the Project Steering Committee
Co-Sponsor	Laura Clark	Chief Security Officer	Active participation in the Project Steering Committee
Co-Sponsor	Jack Harris	Chief Technology Officer	
Program Lead and Project Manager	Jose Semidei	Project Manager	Oversee the project, make management and prioritization decisions. Partner with contractor for planning, access, issue resolution, schedule workshops and meetings with the State staff and project stakeholders.

Table 2: State contact and sponsors

8. State Resources

a. **Executive Sponsor** will administer the terms of this SOW and serve as the primary contact with regards to the advisement of the execution of work contained in this SOW who will have the authority to act on behalf of the State

b. **Program Lead and Project Manager** will oversee the project, make management and prioritization decisions and work side-by-side with Contractor's team. Additional responsibilities include providing support for planning, access, issue resolution, schedule workshops and meetings with the State staff and project stakeholders.

c. **Project Steering Committee** will oversee the progress of the project. This steering committee will have representation from Contractor. Contractor may conduct periodic quality reviews on the services being delivered and the State will cooperate and participate in such reviews.

d. **Development and Operations SMEs** The State will provide resources from the relevant application development and operations areas to support the assessment, strategy, and pilot phases of the project.

e. **Infrastructure SMEs and Testing SMEs** The State will provide

i. Infrastructure resources to provision test environments
ii. Testing team to complete end to end testing/validation
iii. Infrastructure resources to promote the code to production

9. Contractor Project Contacts

Role	Name
Engagement Executive Mike will have responsibility of managing all State executive leadership relations and will be addressing all leadership issues	Mike Kosonog
Engagement Leader Punit Lochan will have responsibility for Contractor's performance of services under this contract in addition to acting as a subject matter specialist.	Punit Lochan
Cyber Security Senior Advisor Keith Zielenski is a leader in Deloitte's application security practice.. Keith will take a part time role on the engagement to advise DTMB senior leadership on Security strategy and provide quality oversight of the delivery of Contractor's services.	Keith Zielenski
DevSecOps Project Manager The Project Manager will oversee delivery of services and serve as a senior subject matter specialist.	Rangesh Venkatesan
DevSecOps Engineers The DevSecOps Engineers are responsible for coaching, and onboarding applications on DevSecOps lifecycle. Engineers will build onboarding templates through integration of DevSecOps tooling, processes and cyber security integration. The engineers direct the implementation of tools and settings, drives reporting and provides technical cybersecurity guidance to application and development teams. May provide assistance to updating existing processes and procedures.	DevOps Engineer 1, DevOps Engineer 2

Table 3: Contractor team and contacts

10. Contractor Key Personnel

Contractor’s Project Manager will be directly responsible for the day-to-day operations of the Contract. Project Manager will be specifically assigned to the State account, be knowledgeable on the contractual requirements, and respond to State inquires, during the normal business hours. Project Manager will coordinate with State application owners and project managers to plan project related activities.

Contractor may bring SME for a specific training or Dojo as identified by state.

Contractor will provide the State, prior to the assignment to work under this contract, with resumes for all individuals performing services under this contract. Assignment of any subcontractor is subject to the requirements provided in Section 3 of the IT Professional Services Contract Terms

11. Meetings

a. **Weekly Team Meetings** the State and Contractor’s project team will meet weekly to review and discuss, including, but not limited to the following:
   ii. Project status and schedule
   iii. Progress of the project
   iv. Deliverable/work product development
   v. Raise and discuss open risks and issues that may have an impact on project performance

Contractor’s Project Manager will facilitate the meetings, develop and circulate meeting agendas, meeting minutes and save the meeting records to the project’s document repository. Immediately following the weekly review meeting Contractor will update the project plan to reflect the current status. Contractor will provide the updated plan to the State Project Manager for approval.

The State may request other meetings, as it deems appropriate.

12. Reporting

a. **Sprint Status Reports** Contractor will provide the State Program Manager a status report at the end of each sprint cycles that will provide the State with the ability to assess the health of the project and review status items, issues and risks. The status report must be provided to the State 10 business days after the completion of the sprint and saved in the designated project document repository. State will review and provide a disposition for each report submitted within 10 business days, after which it will be considered automatically approved.

b. **Sprint Plan** Contractor will provide DTMB with the Sprint plan for review and approval before the start of each sprint cycle. This will include the prioritized backlog, use case and acceptance criteria.

c. **Other Reports** Other reports as identified in this contract.

SCHEDULE B
Pricing

The delivery of DevSecOps project is a fixed price contract following the fee schedule outlined in Table 4 for a total cost of $546,000, not including optional period (beyond Sprint 4). The pricing for Phase 1 includes all costs, including but not limited to, any one-time or set-up charges, fees, and potential costs under this Statement of Work.

The work detailed within this SOW will be executed in 5 sprints as noted in Section 4.

Billing

The Contractor agrees to use a billing model in accordance with the payment terms set forth in this SOW. The Contractor will invoice the State upon submission of each deliverable according to the fee schedule in Table 4.

The State reserves the right to approve optional additional sprints for an additional cost, as agreed to in the optional section of the fee schedule, table 4, below.

Fee Schedule

Phase 1 (Operate)	Deliverables	Estimated Invoice	Estimated Invoice Date	Fixed Capacity
Sprint 0	• Sprint 0 Status Report • Sprint Plan • Sprint Backlog	$130,000	Week 4	500 Story points
Sprint 1	Sprint 1 Status Report	$104,000	Week 8	480 Story points
Sprint 2	Sprint 2 Status Report	$104,000	Week 12	480 Story points
Sprint 3	Sprint 3 Status Report	$104,000	Week 16	480 Story points
Sprint 4	Sprint 4 Status Report	$104,000	Week 20	480 Story points
Phase 2 (Optional)	**Deliverables**	**Estimated Invoice**	**Estimated Invoice Date**	
Sprint 5	Sprint 5 Status Report	$104,000	Week 24	480 Story points
Sprint 6	Sprint 6 Status Report	$104,000	Week 28	480 Story points
Sprint N	Sprint n Status Report	$104,000	Week n+4	480 Story points

Table 4: Sprint invoicing and payment plan

Story Point Estimation

The contractor will provide t-shirt sizing and story points for the backlog items to help DTMB in prioritizing the user stories in Sprint plan. Sprint backlog will be finalized by the total story points less than or equal to the Sprint capacity.

Invoice Requirements

All invoices submitted to the State must include: (a) date; (b) purchase order number; (c) description of the Services; (d) unit price; and (e) total price. Overtime, holiday pay, and travel expenses will not be paid.

Travel Expenses

Travel expenses, including hotel, mileage, meals, parking, etc. are not authorized under this Contract.

Assumptions

1. The State will provide immediate and continued access to key personnel with access and knowledge of existing policies and procedures that are relevant to this engagement.
2. State will provide 30 day notice at the end of Sprint 3, if they decide to stop onboarding applications after 5 month time period.
3. The State is responsible for organizational communication of project goals and expectation management. In addition, the State is responsible for providing appropriate points of contact (for problem escalation, reporting, etc.) in a timely manner.
4. The services will be performed in accordance with the Statement on Standards for Consulting Services issued by the American Institute of Certified Public Accountants (AICPA). Contractor will provide Contractor’s observations, advice, and recommendations. However, Contractor’s services will not constitute an engagement to provide audit, compilation, review, or attestation services as described in the pronouncements on professional standards issued by the AICPA, and, therefore, Contractor will not express an opinion or any other form of assurance with respect to the State’s system of internal control over financial reporting or its compliance with laws, regulations, or other matters.
5. The State will be responsible for software licenses or other costs associate with tools required for DevSecOps pipeline management, processes and capabilities.
6. Deviation from the Project Assumptions may cause changes to Contractor's schedule, professional fees, expenses, level of effort or otherwise impact Contractor's performance of the Services, and the parties will enter a Change Order to reflect adjustments to the Services and/or pricing for such services as a result thereof.
7. Any decisions to be made by DTMB will be made promptly and communicated through the Project Manager. The Project Manager shall have all necessary authority to commit DTMB with respect to the subject matter of this Project.
8. Contractor will have no responsibility for the performance of any third-party software or hardware.
9. To the extent Contractor requires data requests, and Contractor and DTMB shall reach agreement on the data being requested, DTMB shall complete the data request within three (3), or a mutually agreed to number of, business days from request. Inability to provide data may present challenges and hinder the project schedule
10. The project schedule shall recognize U.S. holidays as primary and incorporate holidays of other countries as appropriate. Contractor team members can take holidays/vacations as planned, but these days will not be counted as project time. While progress shall continue those days, both DTMB and Contractor shall recognize that certain resources shall be unavailable during those periods.
11. If there are specifications and/or additional acceptance criteria or procedures separate from those defined herein, DTMB and Contractor shall promptly agree to the additions within the first two (2) weeks of the project.
12. Contractor will not be responsible for delay in application onboarding in case of non-availability of State resources/environments/approvals
13. State will be responsible for securing the co-operation from all required third parties in accordance with the project schedule

14. As the contractor team is not implementing the code in production, there is no warranty or post - production support planned as part of the project plan or budget.
15. State is responsible for testing, acceptance and placing the templates/scripts into the State production environment.
16. State will be using same tools as finalized in pilot phase: Appscan for security, ADO (Azure DevOps for release management

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget
525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **3**
to
Contract Number **180000000986**

CONTRACTOR	DELOITTE & TOUCHE LLP
	300 Renaissance Center
	Detroit, MI 48243
	Mark Ford
	313-394-5313
	mford@deloitte.com
	CV0002117

STATE	Program Manager	Jose Semidei	DTMB
		517-241-2661	
		Semideij@Michigan.gov	
	Contract Administrator	Jordan Sherlock	DTMB
		(517) 243-5556	
		SherlockJ@michigan.gov	

CONTRACT SUMMARY

APPSCAN REMEDIATION AND VALIDATION

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
July 30, 2018	December 31, 2018	4 - 1 Year	December 31, 2020

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-Card	☐ PRC	☐ Other	☒ Yes	☐ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☒	1	☐		December 31, 2021

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$2,941,920.00	$0.00	$2,941,920.00

DESCRIPTION

Effective 12/31/2020, the State is exercising the third option year. The revised contract expiration date is 12/31/2021. The States Contract Administrator is also updated to Jordan Sherlock.

All other terms, conditions, specifications and pricing remain the same. Per contractor and agency agreement, and DTMB Procurement approval.

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget
525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **2**
to
Contract Number **180000000986**

CONTRACTOR	DELOITTE & TOUCHE LLP
	300 Renaissance Center
	Detroit, MI 48243
	Mark Ford
	313-394-5313
	mford@deloitte.com
	CV0002117

STATE	Program Manager	Jose Semidei	DTMB
		517-241-2661	
		Semideij@Michigan.gov	
	Contract Administrator	Garrick Paraskevin	DTMB
		(517) 284-6993	
		paraskeving@michigan.gov	

CONTRACT SUMMARY

APPSCAN REMEDIATION AND VALIDATION

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
July 30, 2018	December 31, 2018	4 - 1 Year	December 31, 2019

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-Card	☐ PRC	☐ Other	☒ Yes	☐ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☒	1	☐		December 31, 2020

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$2,941,920.00	$0.00	$2,941,920.00

DESCRIPTION

Effective 9/9/2019, this Contract is incorporating the attached Statement of Work (SOW) which will utilize $1,277,000 in existing funds for Michigan Cyber Security (MCS)'s DevSecOps efforts. In addition, the State is exercising the second option year. The revised contract expiration date is 12/31/2020.

All other terms, conditions, specifications and pricing remain the same. Per contractor and agency agreement, and DTMB Procurement approval.

SCHEDULE A
STATEMENT OF WORK

1. Background and Scope

a. The Department of Technology, Management and Budget (DTMB) is executing this Statement of Work (SOW) under the AppScan Remediation and Validation Contract (#171-180000000986) to assist DTMB with establishing a program to improve the overall security and quality of application development through the introduction of DevSecOps methodologies and provide the capability for DTMB to begin to rapidly respond to and deploy applications changes as needed to address security issues and/or customer needs. This work will evaluate the current state of DevSecOps across State centers of application development, identify a desired target state, develop a training program to develop the necessary skill sets, and conduct a DevSecOps pilot to apply training to the development lifecycle of a selected application. The Contractor must meet the following project objectives: Conduct an assessment of the current state of security capabilities implemented in existing DevSecOps processes and technologies in flight across DTMB and identify gaps with the desired target state.

b. Conduct an assessment of the current state of application development capabilities implemented in existing DevSecOps processes and technologies in flight across DTMB and identify gaps with the desired target state.

c. Conduct an assessment of the current state of automation and deployment of infrastructure in existing DevSecOps processes and technologies in flight across DTMB and identify gaps with desired target dates.

d. Conduct an assessment of the current state of project management capabilities implemented in existing DevSecOps processes and technologies in flight across DTMB and identify gaps with desired target dates.

e. Provide high-level recommendations of tools, processes, and capabilities, and a roadmap that provides a recommended implementation approach to unify DevSecOps practices across DTMB and facilitate adoption. These recommendations shall include suitability for inclusion in existing SUITE, SEM and MiSAP processes.

~~f.~~ Develop a training plan and implement DevSecOps “Dojos” (e.g. trainings and simulations for DTMB) to build awareness and understanding of DevSecOps in support of the long term goal to deploy and sustain a state-wide DevSecOps development methodology based on gaps identified in the assessment.

g. Develop metrics and key performance indicators (KPIs) to measure DevSecOps performance against goals to establish impact and provide visibility for DTMB leadership.

h. Establish and implement a DevSecOps pilot for up to two (2) applications to evaluate the practical implementation and application of DevSecOps skills and demonstrate impacts and benefits of the methodology on the security and quality of the applications in the pipeline.

The State acknowledges that the scope of Contractor’s project activities does not include handling of any protected health information (PHI), personally identifiable information (PII), and/or payment card information (PCI) within the existing systems or applications in the scope of this project.

2. Project Management

Enterprise Project Management Office (EPMO) SUITE Process

Contractor must follow the EPMO standard State Unified Information Technology Environment (SUITE) process or obtain prior State approval to implement modifications. SUITE is a project management methodology used by the State of Michigan.

3. Project Charter and Project Plan

The State and Contractor will jointly draft a project charter. Contractor will create a project plan with input from the State. The project plan will be reviewed by State on a regular basis including bi-weekly Steering Committee meetings. Contractor's Project Manager will maintain the project plan and review with the State in the weekly status meetings identified in Section 11 (a) – Meetings.

a. **Project Charter** will include the organizational structure of the project delivery team with clear delineation of the responsibilities and the reporting relationships between Contractor and State teams.

b. **Project Plan** will be used to track the progress and status of the project and associated deliverables and must include, but not be limited to, the following:
   i. Breakdown showing the detailed listing of all the activities that will be performed as part of the project including the project phases, sub-projects, tasks, resources, deliverables and timelines required to complete in-scope activities.
   ii. Detailed tasks for assessment, strategy, and pilot will be included in the project plan. The activities will be accompanied by supplementary details such as the resources performing the activities, the deliverables associated with the activities, the proposed start and end dates of the activities, etc. at a minimum.

4. Approach to DevSecOps Assessment, Strategy, and Pilot

To create an assessment and strategy for the State to transition to a DevSecOps model, the following steps will be performed.

Task and Timing	**Activities and Deliverables**
Task 1 – Launch Lab	Contractor will start the project with a "Launch Lab" including one of our senior DevSecOps leaders to educate State leadership and set direction for the overall project. The Launch Lab may take place 2-4 weeks prior to field work beginning for Task 2. Activities: • Conduct a one day immersive learning and alignment experience for 5-7 participants, including the director of each of the four major IT divisions within DTMB, in addition to a DTMB executive(s) (ie – Director, Chief Deputy Director, or CIO) to cover the following agenda: o Identify current pain points o Walk through DevSecOps use cases o Look at current vs future state for people, processes, and technology o Roadmap and set major milestones o Determine next steps Deliverable: Launch Lab Report

Task 2 – DevSecOps Maturity Assessment	Contractor will survey and interview the following 26 groups at the State: 1. (3) business customers one for each of three applications to be determined in advance by the State 2. DTMB PMO 3. Business unit PMO 4. Enterprise Architecture 5. The following groups for the three applications designated by the State (total of 15) a. Business Analysts b. Development Team c. Test Team d. Policy & Compliance e. Independent Verification & Validation 6. Infrastructure Services 7. Telecommunications 8. Security 9. Operations 10. Shared Solutions (including e-Michigan and GIS) Prior to the start of Task 2, Contractor will send stakeholder teams a list of questions that will be used to facilitate maturity assessment. Activities: • Assess and analyze organizational structure of current software development delivery model in the context of transitioning to DevSecOps delivery; • Assess and analyze current state software development and systems provisioning delivery model in the context of a DevSecOps transition. Assessment may include provisioning pipeline, compute asset suitability ranking for DevSecOps use; • Assess current state operations and processes compared to industry standard frameworks for DevSecOps, including software toolchain implementations; • Create and analyze cross organizational view of software development and system delivery model and assess strengths and gaps using benchmarks, inputs and best practices in place at private and public sector organizations that have implemented a DevSecOps delivery model; • Assess current state source control, build process, automated testing and deployment model in the context of a DevSecOps delivery transition; • Assess current code sharing practices to include DTMB developed sharable code modules and the use of open source code; • Assess current state instrumentation, monitoring, automation and cyber control capabilities in the context of a DevSecOps delivery transition; Identify organizational, cultural and structural challenges and recommended changes necessary to implement DevSecOps delivery. • Assess culture of learning and change to understand how we can mature to enterprise DevSecOps practices. Deliverables: Project Charter and Plan DevSecOps Maturity Assessment Report

Task 3 – DevSecOps Strategy and Roadmap	Activities: • Develop an execution “roadmap” to the desired DevSecOps delivery end state to include type of service(s) recommended for DevSecOps support, recommendations for separation from or conversion of existing processes and approaches, and decision trees for DevSecOps transition of various current state processes. • Address governance, process, people, and technology required to adopt a DevSecOps approach to development • Address governance, organizational and culture changes needed to sustain a DevSecOps approach into the future. • Identify tools and skills gap required to adopt DevSecOps across all departments Deliverable: DevSecOps Strategy and Roadmap
Task 4 – DevSecOps Training Dojos	Activity: • Work with leadership to identify training candidates for initial rounds of training to support pilot and rollout of DevSecOps pipeline. • Develop and deliver training and simulation materials to address skills and knowledge gaps identified in maturity assessment including security vulnerability remediation. Deliverable: DevSecOps Training Materials
Task 5 – DevSecOps Metrics and KPIs	Activity • Develop appropriate metrics and KPIs that can be implemented for current DTMB development processes in order to provide a mechanism that will allow DTMB to measure increase in performance over time as DevSecOps processes are deployed to program areas and gain maturity. • Measure DevSecOps delivered system performance against DevSecOps goals for critical measures as recommended e.g. delivery time, defect rate, monitored attributes, infrastructure resource utilization and problem response times; Deliverable: DevSecOps Metrics and KPIs Design
Task 6 – DevSecOps Pilot	The State will identify Pilot applications, participants and stakeholders at least two weeks prior to starting Task 6. Contractor will work with the State to define expected time commitment prior to the start of Task 6. State will have necessary development environments and tools in place prior to Contractor starting Task 6. Activities: • Select three development teams or devops teams for pilot of proposed DevSecOps roadmap. Selected teams may be from other areas within the value stream for software creation, e.g. infrastructure • Conduct senior leadership workshops with resource managers and product owners to develop and prioritize a recommended set of use cases to best leverage assets and capabilities for an initial DevSecOps delivery pilot; • Assess current DevSecOps change efforts and recommend specific Application Development target(s) for a Proof of Concept (PoC) of the recommended DevSecOps delivery implementation;

	• Identify the IT platform candidates for PoC and pilot(s) efforts, including IaaS/PaaS components and approach, and software toolchains for source control, code promotion, build automation, automated testing and instrumentation; • Identify and assist with launch of proof of concept(PoC)/pilot program to demonstrate the concepts, processes and technologies including security test automation, triage, reporting and remediation; • Baseline delivery and performance metrics for PoC/Pilot; • Evaluate tool chains and promotion processes used in PoC/Pilot and identify gaps and strengths of the implemented model • Evaluate and validate consistency of code, configurations, environments, instrumentation and controls for PoC/Pilot(s) delivered using the recommended DevSecOps model • Contractor to advise State on vulnerability remediation strategies for vulnerabilities identified during testing processes • Contractor will provide monthly pilot status report deliverables for 5 months and a final summary of overall pilot effort at the conclusion of the pilot • Provide strategic oversight and evaluation of execution of the Pilot • Leadership Workshops at key milestones • Pilot Summary Report to include: o High level recommendations to existing SUITE, SEM, MiSAP, and SADLC processes to support DevSecOps adoption. o Communications and stakeholder engagement recommendations o Short term and long term recommendations for sustainability o Summary of Pilot accomplishments and opportunities for improvement o Potential project roadmap Deliverables: DevSecOps Pilot Status Report 1 DevSecOps Pilot Status Report 2 DevSecOps Pilot Status Report 3 DevSecOps Pilot Status Report 4 DevSecOps Pilot Status Report 5 DevSecOps Pilot Summary Report

The tasks described above will take place according to the following timeline. Exact activity and deliverable dates will be detailed in the Project Charter and Plan deliverable due to the State by the end of project week 3. Task durations are approximate and may vary from the chart below depending on exact scope of Pilot.

	Week																																		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
Task 1 - Launch Lab	🟦																																		
Task 2 - DevSecOps Maturity Assessment			🟧	🟧	🟧	🟧	🟧	🟧																											
Task 3 - DevSecOps Strategy and Roadmap									🟨	🟨																									
Task 4 - DevSecOps Training Dojos											🟦	🟦																							
Task 5 - DevSecOps Metrics and KPIs											🟪	🟪																							
Task 6 - DevSecOps Pilot													🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

5. Staffing

a. **Work Hours** Contractor will primarily work during State business hours Monday – Friday from 8:00am to 5:00pm Eastern time but may also work outside of these hours and on weekends.

b. **Work Location** Contractor will work primarily from State or Deloitte offices in the Lansing, MI area but may also work remotely as long as work is performed within the United States. The State will provide office space for Contractor's team.

6. State Project Contacts

Role	Name	Title
Executive Sponsor	Chris DeRusha	Chief Security Officer
Co-Sponsor	Jack Harris	Chief Technology Officer
Co-Sponsor	Cindy Peruchietti	DTMB Deputy Director, Agency Services
Delegate Co-Sponsor	Andrew Mason	DTMB Agency Services General Manager
Delegate Co-Sponsor	Jodi Simon	DTMB Agency Services Chief of Staff
Delegate Co-Sponsor	Jim Hogan	DTMB Agency Services General Manager
Program Lead and Project Manager	Jose Semidei	Program Manager – MCS

7. State Resources

a. **Program Lead and Project Manager** The State Program Lead and Project Manager will oversee the project, make management and prioritization decisions and work side-by-side with Contractor's team. Additional responsibilities include providing support for planning, access, issue resolution, schedule workshops and meetings with the State staff and project stakeholders.

b. **Project Steering Committee** The State will establish a project steering committee to oversee the progress of the project. This steering committee will have representation from Contractor. Contractor may conduct periodic quality reviews on the services being delivered and the State will cooperate and participate in such reviews.

c. **Development and Operations SMEs** The State will provide resources from the relevant application development and operations areas to support the assessment, strategy, and pilot phases of the project.

8. Contractor Project Contacts

Role	Name Title

Engagement Leader Punit Lochan will have responsibility for Contractor's performance of services under this contract in addition to acting as a subject matter specialist.	Punit Lochan Managing Director, Deloitte Consulting LLP
DevSecOps Senior Advisor Doug Schneider is the leader of Deloitte's DevSecOps consulting practice for government clients Doug will take a part time role on the engagement to advise DTMB senior leadership on DevSecOps strategy and provide quality oversight of the delivery of our services.	Doug Schneider Managing Director, Deloitte Consulting LLP
DevSecOps Engagement Manager (Key Personnel) The Engagement Manager will oversee delivery of services and serve as a senior subject matter specialist.	Delane Roberts Specialist Master, Deloitte Consulting LLP
DevSecOps Architect The DevSecOps Architect is responsible for leading the development of the Continuous Integration/Continuous Delivery (CI/CD) provides leadership for building quality and security into the tools and processes of in the DevSecOps lifecycle. The DevSecOps Architect will address code libraries, automated testing best practices and release management. Additionally this role will oversee pipeline by identifying security requirements, planning, implementing and testing security controls and procedures.	tbd
DevSecOps Engineers The DevSecOps Engineers integrate technical and cultural/process changes to integrate security in the DevSecOps lifecycle. The engineers directs the implementation of tools and settings, drives reporting and provides technical cybersecurity guidance to application and development teams. May provide assistance to updating existing processes and procedures.	2 resources tbd
Security & Compliance Lead The Security & Compliance Lead will lead the technical and cultural integration of security in the DevSecOps lifecycle. The Lead provides cybersecurity technical thought leadership, guiding security integration for the CI/CD pipeline, and injecting secure coding standards and measurement practices into the DevSecOps lifecycle.	tbd
Security Test Automation Lead The Security Test Automation Lead Leads the integration of security test automation and reporting in the DevSecOps lifecycle. The Lead provides cybersecurity technical thought leadership, guiding the selection and integration of test automation tools for the CI/CD pipeline, and providing guidance on triage, grouping and reporting practices into the DevSecOps lifecycle.	tbd
Engagement Advisors Provide ongoing thought leadership on the execution methodology and analysis of lessons learned from the assessment, strategy, and pilot efforts. In addition to helping our DevSecOps specialists navigate and succeed at the State, Contractor will provide subject matter knowledge as needed with respect to future sustainability of development and operations processes, ongoing monitoring of	Mark Ford Principal, Deloitte & Touche LLP James Shaw VP Service Delivery, Deloitte & Touche LLP

completed work, and validation of completed project deliverables. Contractor will also support various project management activities and identifying the best available resources to execute the project activities.	

9. Contractor Key Personnel

Delane Roberts is Contractor's Project Manager who will be directly responsible for the day-to-day operations of the Contract ("Key Personnel"). Delane Roberts will be specifically assigned to the State account, be knowledgeable on the contractual requirements, and respond to State inquires, during the normal business hours. Delane Roberts will coordinate with State application owners and project managers to plan assessment and pilot activities. In addition to Delane Roberts, the Contractor team will be onsite to facilitate the assessment, strategy, and pilot execution.

Contractor will provide the State, prior to the assignment to work under this contract, with resumes for all individuals performing services under this contract. Assignment of any subcontractor is subject to the requirements provided in Section 3, f of the IT Professional Services Contract Terms

10. Meetings

a. **Weekly Team Meetings** The State and Contractor's project team will meet weekly to review and discuss, including, but not limited to the following:
   i. Weekly 4-up report (or similar)
   ii. Project status and schedule
   iii. Progress of the team
   iv. Deliverable/work product development
   v. Raise and discuss open risks and issues that may have an impact on project performance

Contractor's Project Manager will facilitate the meetings, develop and circulate meeting agendas, meeting minutes and save the meeting records to the project's document repository. Immediately following the weekly review meeting Contractor will update the project plan to reflect the current status. Contractor will provide the updated plan to the State Project Manager for approval.

The State may request other meetings, as it deems appropriate.

11. Reporting

a. **Weekly Status Reports** Contractor must provide the State Program Manager a weekly status report and monthly status report (4-up or similar) to include at a minimum the following: weekly accomplishments, planned activities, potential issues/risks, outstanding items and schedule/scope changes. The status report must be provided on the last working day of the week and Contractor must save the weekly report to the designated project document repository.

b. **Monthly Status Reports** Contractor will provide the State Program Manager a monthly status report that will provide the State with the ability to assess the health of the project and review status items, issues and risks. The status report must be provided to the State by the last working day of the month and saved in the designated project document repository.

c. **Other Reports** Other reports as identified in this contract.

SCHEDULE C
Pricing

This is a fixed price contract and the pricing below include all costs, including but not limited to, any one-time or set-up charges, fees, and potential costs under this Contract.

The work under this SOW will be executed in two phases: 1) DevSecOps Assessment and Roadmap 2) DevSecOps Pilot.

Phase	Price
Launch Lab	$0
DevSecOps Assessment and Strategy (8 weeks)	$285,000
DevSecOps Pilot (23 weeks)	$992,000

Fee Schedule

Deliverables will be billed after acceptance by State, generally expected to be five to ten days after submission, depending on resolution of State’s feedback on deliverables by Contractor.

Phase	Deliverable	Payment	Anticipated Deliverable Submission Date
Launch Lab	Launch Lab Report	$0	Week 1
DevSecOps Assessment and Strategy			
	Project Charter and Plan	$50,000	Week 3
	DevSecOps Maturity Assessment Report	$120,000	Week 10
	DevSecOps Strategy and Roadmap	$115,000	Week 10
DevSecOps Pilot			
	DevSecOps Training Materials	$75,000	Week 12
	DevSecOps Metrics and KPIs Design	$75,000	Week 12
	DevSecOps Pilot Status Report 1	$150,000	Week 16
	DevSecOps Pilot Status Report 2	$150,000	Week 20
	DevSecOps Pilot Status Report 3	$150,000	Week 24
	DevSecOps Pilot Status Report 4	$150,000	Week 28
	DevSecOps Pilot Status Report 5	$150,000	Week 32
	DevSecOps Pilot Summary Report	$92,000	Week 35

The engagement will start September 30, 2019 and run up to June 12, 2020. (35 weeks of work over 37 weeks, assumes two non-working week in December for Christmas holiday).

Deliverable Acceptance and Terms of Payment will be performed as per Sections 12 and 13 of the Contract, with the exception that the State Review Period for this SOW will be defined as 10 business days.

Invoice Requirements

All invoices submitted to the State must include: (a) date; (b) purchase order number; (c) description of the Services; (d) unit price; and (e) total price. Overtime, holiday pay, and travel expenses will not be paid.

Contractor may invoice the State monthly following the State approval of the deliverables identified above.

Travel Expenses

Travel expenses, including hotel, mileage, meals, parking, etc. are not authorized under this Contract.

Assumptions

1. The State will provide immediate and continued access to key personnel with access and knowledge of existing policies and procedures that are relevant to this engagement.
2. The State is responsible for organizational communication of project goals and expectation management. In addition, the State is responsible for providing appropriate points of contact (for problem escalation, reporting, etc.) in a timely manner.
3. The services will be performed in accordance with the Statement on Standards for Consulting Services issued by the American Institute of Certified Public Accountants (AICPA). We will provide our observations, advice, and recommendations. However, our services will not constitute an engagement to provide audit, compilation, review, or attestation services as described in the pronouncements on professional standards issued by the AICPA, and, therefore, we will not express an opinion or any other form of assurance with respect to the State's system of internal control over financial reporting or its compliance with laws, regulations, or other matters.
4. The State will be responsible for software licenses or other costs associate with tools required for DevSecOps pipeline management, processes and capabilities.

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget

525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **1**
to
Contract Number **171180000000986**

CONTRACTOR	DELOITTE & TOUCHE LLP
	300 Renaissance Center
	Detroit, MI 48243
	Mark Ford
	313-394-5313
	mford@deloitte.com
	CV0002117

STATE	Program Manager	Jose Semidei	DTMB-IT
		517-241-2661	
		Semideij@Michigan.gov	
	Contract Administrator	Garrick Paraskevin	DTMB
		(517) 284-6993	
		paraskeving@michigan.gov	

CONTRACT SUMMARY

APPSCAN REMEDIATION AND VALIDATION

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
July 30, 2018	December 31, 2018	4 - 1 Year	December 31, 2018

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS	EXTENDED PURCHASING
☐ P-Card ☐ PRC ☐ Other	☒ Yes ☐ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☒		☐		December 31, 2019

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$2,941,920.00	$0.00	$2,941,920.00

DESCRIPTION

Effective 12/14/2018, this Contract is exercising the first option year and is incorporating the attachment relating to changes to the Phase 1 approach (modifcations are denoted by a yellow highlight). The revised contract expiration date is 12/31/2019.

All other terms, conditions, specifications and pricing remain the same. Per contractor and agency agreement, and DTMB Procurement approval.

SCHEDULE A
STATEMENT OF WORK

1. Background and Scope

The Department of Technology, Management and Budget (DTMB) is executing this contract to conduct work to identify and remediate vulnerabilities through application scanning, remediation and validation of commercial and internally developed applications supporting multiple platforms and technology. The Contractor must meet the following project objectives:

a. Establish and execute a formal project delivery framework with full life cycle rigor and governance.
b. Utilize the DTMB Application Security methodology – Secure Application Development Lifecycle or SADLC, or define a methodology, of equal or more advanced to the DTMB methodology, to be followed for all in scope applications.
c. Develop remediation plans, timelines, resource plans.
d. Remediate (for applications the State has access to source code for) or suggest remediation or configuration options (for 3rd party controlled applications) to address high and medium rated vulnerabilities for in-scope applications from vulnerabilities discovered with the agreed to scanning tool(s).

The State acknowledges that the scope of Contractor's project activities does not include handling of any protected health information (PHI), personally identifiable information (PII), and/or payment card information (PCI) within the existing systems or applications in the scope of this project.

2. Project Management

Enterprise Project Management Office (EPMO) SUITE Process

Contractor must follow the EPMO standard State Unified Information Technology Environment (SUITE) process or obtain prior State approval to implement modifications. SUITE is a project management methodology used by the State of Michigan.

3. Project Charter and Project Plan

Contractor will develop and work with the State project manager to obtain State approval of a detailed project plan and charter within 30 calendar days from the date both parties execute the contract. Contractor will complete this project plan in parallel to the remediation and validation efforts of the 15 applications identified under this initial statement of work. Once approved by the State, Contractor will socialize the project plan and charter with State stakeholders. Contractor's Project Manager, Mark Wireman, will maintain the project plan and review with the State in the weekly status meetings identified in Section 12 (a). Meetings.

a. **Project Charter** will include the organizational structure of the project delivery team with clear delineation of the responsibilities and the reporting relationships between Contractor and State teams.

b. **Project Plan** will be used to track the progress and status of the project and associated deliverables and must include, but not be limited to, the following:

   i. Breakdown showing the detailed listing of all the activities that will be performed as part of the project including the project phases, sub-projects, tasks, resources, deliverables and timelines required to fully complete all remediation and validation efforts. Detailed tasks for remediation, testing and validation exercises will also be included in the project plan. The activities will be accompanied by supplementary details such as the resources performing the activities, the deliverables associated with the activities, the proposed start and end dates of the activities, etc. at a minimum.

4. Approach to Application Scanning, Remediation, and Validation

For each application to be remediated and validated the State and Contractor will complete the following:

Task and Timing	**Milestones and Deliverables**
Task 1 – Application Scanning, Deconstruction, and Vulnerability Identification Timing: Completed within 8 weeks of engagement start Owner: State	The State will dynamically or statically scan all applications utilizing the DTMB Enterprise Application Scanning platform – IBM AppScan to identify vulnerabilities. If another method of testing is required to ascertain the root cause of vulnerabilities, the State will determine if additional testing tools will be used.
Task 2 – Vulnerability Analysis and Remediation Work Plan Timing: 9 weeks from contact execution date Owner: Contractor and State	The State's central scanning function will provide application architecture and design, dynamic application security testing ("DAST") results, manual penetration testing results, and static application security testing ("SAST") analysis results. The State will reconcile findings and create a definitive prioritized list of vulnerabilities in the order of assigned severity to be remediated. The State will provide this information to Contractor along with information describing how the application interacts with external entities; use-cases to understand how the application is used, and the identification of entry points to see where a potential attacker could interact with the application, identifying assets, i.e. items/areas that the attacker would be interested in, and identifying trust levels which represent the access rights that the application will grant to external entities. Contractor will review vulnerabilities from the State's central scanning function. The State will conduct a preliminary false positive analysis. Contractor, in conjunction with the state development team and review with state app scan team, will conduct a false positive analysis of the identified vulnerabilities and scan the code base. .

Contractor will then develop the remediation work plan. The remediation work plan must include the following:

a. Review and determine severity and priority for vulnerabilities
b. Recommend vulnerabilities to be remediated
c. Recommend existing compensating controls that can remediate the vulnerability
d. Remediation approach, including testing procedures to analyze that security vulnerabilities have been remediated
e. Risk mitigation strategy
f. Tasks, dependencies, resources, timelines, etc.
g. Expected results
h. Identification of level of effort to remediate (see Table 1 in Pricing) and amount of time needed to remediate

The Remediation Work Plan must enumerate vulnerabilities and remediation tasks across the following:

Common system architecture risk areas:

a. Authentication
b. Session Management
c. Error Handling and Logging
d. Hypertext Transfer Protocol (HTTP) Security
e. Malicious Controls

Common application risk areas, or open web application security project ("OWASP") top ten (10):

a. A1: Injection
b. A2: Broken Authentication and Session Management
c. A3: Cross-Site Scripting ("XSS")
d. A4: Insecure Direct Object References
e. A5: Security Misconfiguration
f. A6: Sensitive Data Exposure
g. A7: Missing Function Level Access Control
h. A8: Cross Site Request Forgery ("CSRF")
i. A9: Using Components and Known Vulnerabilities
j. A10: Un-validated Redirects and Forwards

Contractor must provide key developers and vulnerability specialists to remediate identified vulnerabilities. Contractor will only act in a coordinator role for applications where Contractor is not permitted to modify code (e.g. COTS products, or applications currently maintained by other vendors).

Contractor must obtain State approval for the remediation work plan, including application type for each application. Upon State approval, Contractor will conduct project kick-off meeting with the stakeholders to communicate the remediation work plan, expectations, schedule, etc.

Task 3 – Remediation and Resolution Validation Report Timing: 26 weeks from contract execution date. Owner: Contractor	When available and applicable (e.g. State owned/maintained applications) the State will provide Contractor with on-demand (during business hours) access to the following: a. Code bases and ability to remediate application code b. Design documents or other relevant documents, templates and related material and ability to update design documents c. Development environment and access to promote code d. Test environments or follow a process to promote code e. Production environments or follow a process to promote code f. Application administrator console or will be provided a Subject Matter Expert/Admin g. Remote Virtual Private Network (VPN) access on a 24x7 basis to the project environment h. Key application team personnel with access and knowledge of existing policies and procedures that are relevant to this contract i. Relevant hardware, software, licenses, etc. and appropriate relate setup/maintenance/support for developing project deliverables. For applications where access to all application components is available: a. Perform modification to application source code in the development environment b. Perform modification to application configuration settings in the development environment c. Perform modification to infrastructure configuration settings in the development environment (in conjunction with State resources if needed) d. In conjunction with Michigan Cyber Security and Telecom, perform modification to compensating controls (i.e. Firewalls, Web Application Firewalls, Access Control) The State will promote code and configuration settings into higher environments and perform testing. For applications where access to one or more application components is not available: a. Provide guidance and remediation assistance to each respective application development team to remediate vulnerabilities associated with the source code. b. Provide guidance and assistance to the appropriate application architecture/infrastructure teams to remediate system configuration related vulnerabilities.

	For system/architecture vulnerabilities, Contractor will complete the following: a. Recommend and coordinate configuration changes and other compensating controls at the system/architecture level to address vulnerabilities across the in-scope applications. b. Recommend and coordinate additional remaining configuration changes and other compensating controls at the system/architecture level specific to one or more of the in-scope applications. c. The State will implement agreed upon configuration changes. For application specific vulnerabilities, Contractor will complete the following tasks where applicable: a. In coordination with each of the development teams, implement code changes or mitigating controls to address the identified vulnerabilities. b. Assist the application development team for reviewing software source code to identify code modifications required to remediate identified vulnerabilities in the in-scope applications. c. Assist in remediating identified vulnerabilities in software source code. d. Review and assess original source code from the application team's version control system. e. Modify source code to resolve identified vulnerabilities, based on approval and review of requirements and criteria by application team's personnel. • Submit source code changes to application team's version control system. • Perform remediation of application code to the in-scope applications. • Whenever possible, use standard, repeatable code or routines to remediate vulnerabilities. • Provide static code analysis to the team to analyze whether the changes have addressed the identified vulnerabilities. For all applications where a remediation plan is executed Contractor will complete the following: a. For .NET apps: • Update the common .NET Developer cookbook in SharePoint • Add any OWASP related links to the OWASP Links library • Add any .NET or Microsoft related links to the .NET Links library • Add any .NET or Microsoft related docs to the .NET Documents library • Add any .NET or Microsoft Code in a .ZIP file with context verbiage in the .NET Secure Code Wiki

	b. For Java apps: • Update the Java Developer cookbook in SharePoint • Add any OWASP related links to the OWASP Links library • Add any Java related links to the Java Links library • Add any Java related docs to the Java Documents library • Add any Java Code in a .ZIP file with context verbiage in the Java Secure Code Wiki Contractor must update the State DTMB Developer Application Security Best Practice Cookbook (DASBPC), to support cross team utilization of solutions. Update to include OWASP links, specific language links and documents and upload any reusable code in WIKI pages. Contractor must provide a report describing the outcome of executing the vulnerability remediation plans ("Resolution Validation Report"). The Resolution Validation Report must include documentation of remediation activities performed and the outcomes achieved, system architecture changes and exceptions, and that the update to the DASBPC has been completed. The Resolution Validation Report will be an artifact within the Remediation Validation Report deliverable. Vulnerabilities or defects identified in commercial software products are the State's responsibility to resolve. It is the State's responsibility to install, test, and implement software patches to address vulnerabilities identified in commercial software products.
Task 4 - Retesting After Remediation Timing: Each application to be retested within two weeks of remediation performed under Task 3 Owner: State and the Contractor	After Contractor provides the State with the Resolution Validation Report, the State will re-run the scan to validate the remediation is complete and the State will determine if additional remediation efforts will be conducted. Any additional remediation efforts will follow the process identified in Section 3, Approach to Application Scanning, Remediation and Validation. Once the remediation for the agreed upon number of vulnerability types has been completed any future testing and remediation efforts would be considered out of scope and need to be handled through a change request. After completion of Task 4 and the State's approval of code changes and recommendations Contractor will have no responsibility or liability for any recommended configuration changes or custom code developed to address State identified vulnerabilities in the in-scope applications.
Task 5 - Create Backlog for Developers Timing: Within one week of each	After re-testing, Contractor will arrive at a reasonable set of vulnerabilities that the State will report into the Plan of Action & Milestone (POA&M) process or similar, particularly for vulnerability that may require longer resolution time. To enable this, Contractor will create a backlog into which we load all the vulnerabilities and hand it over to the developers to start the long-term process of them caring for the vulnerability management of their application.

application retesting in Task 4 and 5 Owner: Contractor	
Task 6 - Education and Cultural Change Timing: 1 day Owner: Contractor	Contractor will educate and provide a controlled set of rules and training on how to securely develop application code to be reused by the State with up to two three-hour learning sessions.

Illustrative timeline – may be modified by mutual agreement of Contractor and State.

	Week																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Task 1 - Scanning	🟦	🟦	🟦	🟦	🟦	🟦	🟦													
Task 2 - Analysis	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧											
Task 3 - Remediation			🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨		
Task 4 - Retesting					🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
Task 5 - Developer Backlog					🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪
Task 6 - Education and Culture Change																🟩				

5. Staffing

a. **Work Hours** Contractor will provide the Services during the State's normal working hours Monday – Friday 8:00 am to 5:00 pm, Eastern Standard time, and evenings and weekends. The work schedule will be determined by the State and will depend on the specific remediation efforts and potential business impact.

b. **Work Location** Lansing, MI, and as approved, some work may be performed off-site, but must be within the United States. The State will provide office space for Contractor's team.

6. State Project Contacts

Role	Name	Title
Executive Sponsor	Rajiv Das	Deputy Director and Chief Security Officer
Co-Sponsor	Rodney Davenport	Deputy Director and Chief Technology Officer
Co-Sponsor	Tiziana Galeazzi	Acting Deputy Director – Agency Services
Program Lead and Project Manager	Jose Semidei	Program Manager – MCS Contact Number **517-241-2261**

7. DTMB Application Scanning System Administrator

The State will provide Contractor with access to the DTMB Application Scanning System Administrator

8. DTMB Application and Infrastructure SME

The State will provide subject matter experts for customer and infrastructure applications.

9. State Resources

a. **Program Lead and Project Manager** The State Program Lead and Project Manager will oversee the project, make management and prioritization decisions and work side-by-side with Contractor's team. Additional responsibilities include providing support for planning, access, issue resolution, schedule workshops and meetings with the State staff and project stakeholders.

b. **Project Steering Committee** The State will establish a project steering committee to oversee the progress of the project. This steering committee will have representation from Contractor. Contractor may conduct periodic quality reviews on the services being delivered and the State wil cooperate and participate in such reviews.

10. Contractor Project Contacts

Role	Name Title
Engagement Leader Ultimate responsibility for Contractor's performance of services under this contract in addition to acting as a subject matter specialist	Mark Moore, Managing Director, Deloitte & Touche LLP
Vulnerability Specialist and Project Manager (Key Personnel and will be on site) Run the day to day activities of Contractor's project team and assist with various project management activities as well as developing the vulnerability remediation strategy for the in-scope applications.	Mark Wireman, Specialist Leader, Deloitte & Touche LLP
Senior Vulnerability Remediation Specialist Will work under Mark Wireman's direction to perform the analysis, remediation and validation tasks.	Mechelle McGowan, Senior Consultant, Deloitte & Touche LLP
Vulnerability Remediation Specialist Will work under Mark Wireman's direction to perform the analysis, remediation and validation tasks.	Specific resources to be confirmed during analysis phase of the project
Vulnerability Remediation Developers Will work under Mark Wireman's direction to perform application remediation tasks.	Specific resources to be confirmed during analysis phase of the project

Engagement Advisors Provide ongoing thought leadership on the execution methodology and analysis of lessons learned from the remediation and validation efforts, as well as provide guidance and thought leadership on how to implement security, patching, and monitoring controls throughout the State IT infrastructure. Assist the project team assimilate into the State's culture and working environment.	Mark Ford, Principal, Deloitte & Touche LLP
Engagement Advisor In addition to helping our vulnerability remediation specialists navigate and succeed at the State, will provide subject matter knowledge as needed with respect to future sustainability of control processes, ongoing monitoring of completed work, and validation of completed remediation efforts. James will also support various project management activities and identifying the best available resources to execute the remediation activities.	James Shaw, Senior Manager, Deloitte & Touche LLP

11. Contractor Key Personnel

Mark Wireman is Contractor's Project Manager who will be directly responsible for the day-to-day operations of the Contract ("Key Personnel"). Mark Wireman must be specifically assigned to the State account, be knowledgeable on the contractual requirements, and respond to State inquires, and be on-site in Lansing, MI during the normal business hours. Mark Wireman will coordinate with State application owners and project managers to plan remediation, validation and retesting activities. In addition to Mark, the Contractor team will be onsite to complete remediation, validation and retesting activities.

Contractor will provide the State, prior to the assignment to work under this contract, with resumes for all individuals performing services under this contract. Assignment of any subcontractor is subject to the requirements provided in Section 3, f of the IT Professional Services Contract Terms.

12. Meetings

a. **Weekly Team Meetings** The State and Contractor's project team will meet weekly to review and discuss, including, but not limited to the following:
   - **i.** Weekly 4-up report
   - ii. Project status and schedule
   - iii. Progress of the team
   - iv. Deliverable/work product development
   - v. Raise and discuss unresolved issues that may have an impact on project performance

Contractor's Project Manager will facilitate the meetings, develop and circulate meeting agendas, meeting minutes and save the meeting records to the project's document repository. Immediately following the weekly review meeting Contractor will update the project plan to reflect the current status. Contractor will provide the updated plan to the State Project Manager for approval.

The State may request other meetings, as it deems appropriate.

13. Reporting

a. **Weekly Status Reports** Contractor must provide the State Program Manager a weekly status report and monthly status report (4-up or similar) to include at a minimum the following: weekly accomplishments, planned activities, potential issues/risks, outstanding items and schedule/scope changes. The status report must be provided on the last working day of the week and Contractor must save the weekly report to the designated project document repository.

b. **Monthly Status Reports** Contractor will provide the State Program Manager a monthly status report that will provide the State with the ability to assess the health of the project and review status items, issues and risks. The status report must be provided to the State by the last working day of the month and saved in the designated project document repository.

c. **Other Reports** Other reports as identified in this contract.

14. Oath of Office

Department of Insurance and Financial Services will require Contractor and all employees and subcontractors to take an Oath of Office before beginning work. This oath ensures that employees and contractors who have access to the Department of Insurance and Financial Services regulatory information keep the information confidential.

SCHEDULE B
High Value Applications

This schedule identifies the initial 14 applications that Contractor must complete (Tasks 2-3 identified in **Section 4, Approach to Application Scanning, Remediation, and Validation)** within

90 business days following the date the State provides Contractor with the requirements of Task 1 of this same Section.

High Value Applications - derived from Red Card Apps	**Program Language**	**Platform**	**Database**	**Code maintained by DTMB or 3rd Party Vendor**	**Approx Lines of code**
MDHHS MiTEAM Fidelity	.NET	Web	Oracle	DTMB Supported	75K
DEQ MiWaters	.NET	Web	SQL Server	Vendor Supported	200K +
Electronic Death Registry System (EDRS)	Java	Web	Oracle	DTMB Supported	746,500
Birth Registry System (BRS)	Java	Web	Oracle	DTMB Supported	500K
CEPI Financial Information Database (FID)	.NET	Web	SQL 2014	DTMB Supported	<100K
Michigan Bridge Management and Inspection System (MiBridge)	Java	Web	Unknown	DTMB Supported	100-500K
Michigan Women Infants and Children (MiWIC)	.NET	Web	Oracle	Vendor Supported	100-500K
Electronic Death Registration System (EDRS)	Java	Web	Unknown	DTMB Supported	500K-<1M
DTMB Enterprise FileNet	.NET	Web	Oracle	Vendor Supported	>1M
Insurance Licensing Online System (ILOS)	.NET	Web	MSSQL Server 2012	DTMB Supported	<100K
DIFS Licensing Express Renewal	.NET	Web	Oracle	DTMB Supported	<100K
DNR Land Ownership Tracking (LOTS)	.NET	Web	MS SQL Server 2014	DTMB Supported	100-500K
MDE Secure Site	.NET	Web	MS SQL Server 2016	DTMB Supported	<100K

DIFS Mi Health Insurance Enrollment	.NET	Web	Oracle	DTMB Supported	<100K
DIFS Education Roster Entry System (ERES)	.NET	Web	Oracle	DTMB Supported	<100K

SCHEDULE C
Pricing

This is a fixed price contract and the pricing below include all costs, including but not limited to, any one-time or set-up charges, fees, and potential costs under this Contract.

The work under this SOW will be executed in two phases: assessment and remediation. The first phase will be to analyze the assessment results provided by the State to Contractor. The pricing for the first phase will be fixed as indicated below for the analysis of the 15 applications listed in Schedule B. During the first phase the applications will be categorized by remediation complexity level to determine the effort and pricing for the remediation phase. Complexity level will be determined using a scoring system that evaluates the effort drivers of the remediation work including: number of programming languages, lines of code, time since the most recent security assessment, application configuration type and other criteria listed below in Pricing Table 1. Application remediation will be performed on a fixed fee basis according to the complexity level and relevant assumptions.

Milestone	Deliverable	Pricing
Assessment Phase - Section 4 Task 2, Vulnerability Analysis and Remediation Work Plans	Bundled State Approved Remediation Work Plans for applications identified in Schedule B	$124,000 for 14 applications
Remediation and Validation Phase Section 4 – Tasks 3-5	Remediation Validation Report and state sign-off on Re-testing for each application	$47,000 per Complex application $36,900 per High application $27,700 per Medium application $23,100 per Low application All Remediation pricing assumes a maximum of 12 unique vulnerability types per application.
Education and Culture Change – Task 6	Development rules and training presentation document and training	No cost

Pricing for worked performed under subsequent statements of work will not exceed the pricing identified in this Statement of Work (e.g. $4285 per application for the Assessment Phase, and the prices identified for the Remediation and Validation Phase) so long as the State provides Contractor with a minimum of 15 applications for each subsequent Statement of Work.

The Task 2 deliverable will be invoiced upon approval of the Task 2 deliverable “Bundled State Approved Remediation Work Plans”.

The Task 3-5 deliverable “Remediation Validation Report and state sign-off on Re-testing for each application” will be invoiced individually at the conclusion of Task 5 for each of the 14 applications.

Total duration of the engagement is 26 weeks or 130 business days, starting on July 30, 2018. Engagement conclusion is dependent on vulnerability remediation and retesting and may result in a finish date sooner than 130 business days. Upon agreement by the State and the Contractor, the timelines may be extended.

The State will have 5 business days to approve deliverables or provide feedback. If not feedback is received after 5 business days deliverables will be considered approved. Contractor will have 5 business days to address feedback received on deliverables.

If more than 12 unique vulnerability types per application are identified and the State wishes to have Contractor fix those additional vulnerability types that work will be billed on a time and material basis according to the following rate card:

Role	**Deloitte Title**	**Hourly Rate**
Engagement Leader	Principal/Managing Director	$ 302
Project Manager	Senior Manager	$ 281
Team Lead	Manager or Solution Manager	$ 262
Vulnerability Management Sr. Specialist	Senior Consultant or Senior Solution Engineer	$ 229
Vulnerability Management Specialist	Consultant or Solution Engineer	$ 198

Pricing Table 1 – Application Remediation Complexity Scoring

	Score	Complexity Level
Infrastructure Scoring		
Fix & Config Change	2	Medium
Fix & No Config Change	1	Low
No Change	0	NIL
COTS App Scoring		
External	3	High

Non-COTS	1	Low
Custom App Scoring		
Greater than 100 modules	4	Complex
50 modules to less than 100 modules	3	High
25 to less than 50 modules	2	Medium
Less than 25 modules	1	Low
Number of Users		
Greater than 10k	4	Complex
5k to less than 10k	3	High
1k to less than 5k	2	Medium
Less than 1k	1	Low
Number of App Languages		
3 or greater languages	4	Complex
2 languages	3	High
1 language	1	Low
Number of Lines of Code		
Greater than 1 Million	4	Complex
500k to less than 1 Million	3	High
100k to less than 500k	2	Medium
Less than 100k	1	Low
Recent Security Assessment (COTS and non-COTS)		
More than 3 years or Never	4	Complex
24 months to less 3 years	3	High
12 months to less than 24 months	2	Medium
Less than 12 months	1	Low
Application Configuration (COTS and non-COTS)		
ERP or SAP	4	Complex
Non-ERP or SAP	1	Low

N-Tier	4	Complex
Non-N-Tier	1	Low
Complex	27+	
High	18+ to 27	
Medium	9 to 18	
Low	8 or less	

Invoice Requirements

All invoices submitted to the State must include: (a) date; (b) purchase order number; (c) description of the Services; (d) unit price; and (e) total price. Overtime, holiday pay, and travel expenses will not be paid.

Contractor may invoice the State monthly following the State approval of the deliverables identified above.

Travel Expenses

Travel expenses, including hotel, mileage, meals, parking, etc. are not authorized under this Contract.

Assumptions

1. Contractor will not be responsible for executing QA, Pre-Deployment, or Deployment activities upon completion of remediation activities.
2. Completed application security scans shall be immediately available and results accessible to the Contractor personnel at the start of the project.
3. Contractor will not verify or validate the efficiency of security tests executed
4. The State of Michigan will provide immediate and continued access to key personnel with access and knowledge of existing policies and procedures that are relevant to this engagement.
5. The State is responsible for organizational communication of project goals and expectation management. In addition, the State is responsible for providing appropriate points of contact (for problem escalation, reporting, etc.) in a timely manner.
6. The services will be performed in accordance with the Statement on Standards for Consulting Services issued by the American Institute of Certified Public Accountants (AICPA). We will provide our observations, advice, and recommendations. However, our services will not constitute an engagement to provide audit, compilation, review, or attestation services as described in the pronouncements on professional standards issued by the AICPA, and, therefore, we will not express an opinion or any other form of assurance with respect to the State's system of internal control over financial reporting or its compliance with laws, regulations, or other matters.
7. Up to 12 unique vulnerabilities per application are assumed for the pricing options provided. Additional vulnerabilities to be analyzed and remediated will be appropriately priced using a change order.

8. The time and materials (T&M) hourly rates for Contractor staff under this Statement of Work shall remain in place for the period of one (1) year following the date of contract execution. The T&M hourly rate corresponding to each staff will be increased by no more than five percent (5%) each year for the duration of the contract, including the possible extension years.
9. Contractor will only modify custom source code controlled by the State. Contractor will not modify commercial software products.
10. The State will be responsible for software licenses or other costs associate with tools required for vulnerability testing or remediation. (e.g. source code repository and development tools).

STATE OF MICHIGAN
ENTERPRISE PROCUREMENT

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

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **171-180000000986**
between
THE STATE OF MICHIGAN
and

CONTRACTOR	Deloitte & Touche LLP
	300 Renaissance Center
	Detroit, MI 48243
	Mark Ford
	313-394-5313
	mford@deloitte.com
	CV0002117

STATE	Program Manager	Jose Semidei	DTMB
		517-241-2661	
		Semideij@michigan.gov	
	Contract Administrator	Garrick Paraskevin	DTMB
		517-256-7516	
		paraskeving@michigan.gov	

CONTRACT SUMMARY			
DESCRIPTION: AppScan Remediation and Validation			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW**
7/30/2018	12/31/2018	4 – 1 year	12-31-2018
PAYMENT TERMS		**DELIVERY TIMEFRAME**	
Net 45		N/A	
ALTERNATE PAYMENT OPTIONS			**EXTENDED PURCHASING**
☐ P-card	☐ Direct Voucher (DV)	☐ Other	☒ Yes ☐ No
MINIMUM DELIVERY REQUIREMENTS			
MISCELLANEOUS INFORMATION			
This contract is established from Direct Solicitation 171-180000000073			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION		**2,941,920.00**	

FOR THE CONTRACTOR:

Deloitte & Touche LLP

Company Name

Authorized Agent Signature

Mark Moore________

Authorized Agent **(Print or Type)**

Date

FOR THE STATE:

Signature

Heather Calahan

Name & Title

DTMB Central Procurement Servcies

Agency

Date

STATE OF MICHIGAN

IT PROFESSIONAL SERVICES

CONTRACT TERMS

This IT Professional Services Contract (the "**Contract**") is agreed to between the State of Michigan (the "**State**") and Deloitte & Touche LLP ("**Contractor**"), a Delaware limited liability partnership. This Contract is effective on July 30, 2018 ("**Effective Date**"), and unless terminated, expires on 12/31/2018 (the "**Term**").

This Contract may be renewed for up to four (4) additional one (1) year periods. Renewal must be by written notice from the State and will automatically extend the Term of this Contract.

The parties agree as follows:

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

"**Affiliate**" United States entities that control, are controlled by, or are under common control with, another entity.

"**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.

"**Confidential Information**" has the meaning set forth in **Section 21a**.

"**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 **Section 5** or an individual Statement of Work.

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

"**Contractor Personnel**" means all employees of Contractor or any Subcontractors involved in the performance of Services and creation of Deliverables under this Contract.

"**Deliverables**" means Work Product, documentation, reports, and all other materials that Contractor or any Subcontractor 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 an individual Statement of Work.

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

"**Financial Audit Period**" has the meaning set forth in **Section 23**.

"**Key Personnel**" means any Contractor Personnel identified as key personnel in this Contract or an individual Statement of Work.

"**Services**" means any of the services Contractor, or any Subcontractor, is required to or otherwise does provide under this Contract, or an individual Statement of Work, as more fully described in this Contract or the applicable Statement of Work.

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

"**State Data**" has the meaning set forth in **Section 10.a.**

"**State Review Period**" has the meaning set forth in **Section 12**.

"**Statement of Work**" has the meaning set forth in **Section 2**.

"**Stop Work Order**" has the meaning set forth in **Section 14**.

"**Subcontractor**" has the meaning set forth in **Section 3.f**.

"**Transition Responsibilities**" has the meaning set forth in **Section 17**.

"**Unauthorized Removal**" has the meaning set forth in **Section 3.e.ii**.

"**Unauthorized Removal Credit**" has the meaning set forth in **Section 3.e.iii**.

"**Work Product**" means all State-specific deliverables that Contractor is required to, or otherwise does, provide to the State under this Contract including but not limited to 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. **Statement of Work**. Contractor shall provide the Services and Deliverables pursuant to a Statement of Work, attached as **Schedule A** to this Contract, and other Statements of Work as the parties mutually agree in writing (the "**Statement of Work**"). The Statements of Work will not be effective unless signed by Contractor and the State's Contract Administrator and incorporated into the Contract pursuant to the Contract Change Control process as outlined in Section 38. The terms and conditions of this Contract will apply at all times to the Statement of Work. The State shall have the right to terminate any Statement of Work, in whole or in part, as set forth in **Sections 15 and 16** of this Contract.

3. **Performance of Services**.

   a. **Performance Warranty**. Contractor represents and warrants that its Services hereunder shall be performed by competent personnel and shall be of professional quality consistent with generally accepted industry standards for the performance of such services and shall comply in all respects with the requirements of this Contract and the specifications and time periods set forth in the applicable Statement of Work. For any breach of this warranty, the State may, at its option, either terminate a Statement of Work pursuant to the termination provision herein if the breach remains uncured for thirty (30) days after the Contractor receives written notice thereof, or require Contractor to provide replacement personnel fully qualified for the position within thirty (30) calendar days of Contractor's receipt of notification from the State. Whether or not the departing Contractor Personnel are to continue working while Contractor attempts to find replacement personnel is at the sole discretion of the State. If Contractor is notified within the first eight (8) hours of assignment that the person is not fully qualified for the position, Contractor will not charge the State for those hours; otherwise, the State shall pay for all actual hours worked prior to the State's notification of a replacement request to Contractor.

   b. **State Standards**

      i. The Contractor must adhere to all existing standards as described within the comprehensive listing of the State's existing technology standards at http://www.michigan.gov/dmb/0,4568,7-150-56355-108233--,00.html

ii. To the extent that Contractor has access to the State's computer system, Contractor must comply with the State's Acceptable Use Policy, see http://www.michigan.gov/dtmb/0,5552,7-150-56355_56579_56755---,00.html. All Contractor Personnel will be required, in writing, to agree to the State's Acceptable Use Policy before accessing the State's system. The State reserves the right to terminate Contractor's access to the State's system if a violation occurs.

c. **Contractor Personnel**

i. 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.

ii. Prior to any Contractor Personnel performing any Services, Contractor will:

1. ensure that such Contractor Personnel have the legal right to work in the United States; and

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

iii. 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.

iv. 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.

d. **Background Checks.** Upon request, Contractor must perform background checks on all employees and subcontractors and its employees prior to their assignment under the applicable Statement of Work, which background checks must comprise, at a minimum, a review of credit history, references and criminal record, in accordance with applicable law. Contractor is responsible for all costs associated with the requested background checks. The State, in its sole discretion, may also perform background checks.

e. **Contractor's Key Personnel**

i. The State has the right to recommend and approve in writing the initial assignment, as well as any proposed reassignment or replacement, of any Key Personnel. Before assigning an individual to any Key Personnel position, Contractor will notify the State of the proposed assignment, introduce the individual to the State's Project Manager, and provide the State with a resume and any other information about the individual reasonably requested by the State. The State reserves the right to interview the individual before granting written approval. In the event the State finds a proposed individual unacceptable, the State will provide a written explanation including reasonable detail outlining the reasons for the rejection.

ii. Contractor will not remove any Key Personnel from their assigned roles on this Contract without the prior written consent of the State. The Contractor's removal of Key Personnel without the prior written consent of the State is an unauthorized removal ("**Unauthorized Removal**"). An Unauthorized Removal does not include replacing Key Personnel for reasons beyond the reasonable control of Contractor, including illness, disability, leave of absence, personal emergency circumstances, resignation, or for cause termination of the Key Personnel's employment, or the promotion or transfer of the Key Personnel, provided that such transfer or promotion occurs after twelve (12) months from the effective date of the final Statement of Work and Contractor identifies a replacement approved by the State and assigns the replacement to shadow the Key Personnel who has been promoted or transferred for a period of at least 30 calendar, unless otherwise specified in the Statement of Work. Any Unauthorized Removal may be considered by the State to be a material breach of this Contract, in respect of which the State may elect to terminate this Contract for cause under **Section 15**.

iii. It is further acknowledged that an Unauthorized Removal will interfere with the timely and proper completion of this Contract, to the loss and damage of the State, and that it would be impracticable and extremely difficult to fix the actual damage sustained by the State as a result of any Unauthorized Removal. Therefore, Contractor and the State agree that in the case of any Unauthorized Removal in respect of which the State does not elect to exercise its rights under **Section 15**Error! Reference source not found., Contractor will issue to the State the corresponding credits set forth below (each, an "**Unauthorized Removal Credit**"):

1. For the Unauthorized Removal of any Key Personnel designated in a Statement of Work, the credit amount will be $25,000.00 per individual if Contractor identifies a replacement approved by the State and assigns the replacement to shadow the Key Personnel who is leaving for a period of at least 30 calendar days before the Key Personnel's removal.

2. If Contractor fails to assign a replacement to shadow the removed Key Personnel for at least 30 calendar days, in addition to the $25,000.00 credit specified above, Contractor will credit the State $833.33 per calendar day for each day of the 30 calendar-day shadow period that the replacement Key Personnel does not shadow the removed Key Personnel, up to $25,000 maximum per individual. The total Unauthorized Removal Credits that may be assessed per Unauthorized Removal and failure to provide 30 calendar days of shadowing will not exceed $50,000.00 per individual.

3. Contractor's aggregate liability for all Unauthorized Removal Credits assessed under all Statements of Work shall not exceed $250,000, which will be the State's exclusive monetary remedy for Unauthorized Removals.

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

f. **Subcontractors**. With the exception of Contractor's affiliates, Contractor will not, without the prior written approval of the State, which consent may be given or withheld in the State's sole discretion, engage any third party to perform Services (including to create any Deliverables). The State's approval of any such third party (each approved third party, a "**Subcontractor**") does not relieve Contractor of its representations, warranties or obligations under this Contract. Without limiting the foregoing, Contractor will:

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

ii. name the State a third party beneficiary under Contractor's contract with each Subcontractor with respect to the Services and Deliverables;

iii. be responsible for all fees and expenses payable to, by or on behalf of each 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

iv. prior to the provision of Services or creation of Deliverables by any Subcontractor, if requested by the State:

1. obtain from such Subcontractor confidentiality, work-for-hire and intellectual property rights assignment agreements, in form and substance acceptable by the State, not to be unreasonably withheld, giving the State rights consistent with those set forth in **Section 9.a** and, upon request, provide the State with a fully-executed copy of each such contract; and

2. with respect to all Subcontractor employees providing Services or Deliverables, comply with its obligations under **subsection c** above.

4. **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:
Garrick Paraskevin Category Analyst, IT Central Procurement Services State of Michigan 517-256-7516 Paraskeving@michigan.gov	Mark Ford 200 Renaissance Center Detroit, MI 48243 313-394-5313 mford@deloitte.com

5. **Contract Administrators.** The Contract Administrator for each party is the only person authorized to modify any terms and conditions of this Contract and are identified below:

State:	Contractor:
Garrick Paraskevin Category Analyst, IT Central Procurement Services State of Michigan 517-256-7516 Paraskeving@michigan.gov	Mark Ford 200 Renaissance Center Detroit, MI 48243 313-394-5313 mford@deloitte.com

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

Insurance Type	Additional Requirements
Commercial General Liability Insurance	
Minimal Limits: $1,000,000 Each Occurrence Limit $1,000,000 Personal & Advertising Injury Limit $2,000,000 General Aggregate Limit $2,000,000 Products/Completed Operations	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 specific to Contractor’s acts or omissions in performance of Services under this Agreement..
Umbrella or Excess Liability Insurance	
Minimal Limits: $5,000,000 per Occurrence/General Aggregate	Contractor must have their policy endorsed to add “the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents” as additional insureds specific to Contractor’s acts or omissions in performance of Services under this Agreement.
Automobile Liability Insurance	
Minimal Limits: $1,000,000 Per Accident	
Workers' Compensation Insurance	
Minimal Limits: Coverage according to applicable laws governing work activities.	Waiver of subrogation, except where waiver is prohibited by law.
Employers Liability Insurance	
Minimal Limits: $100,000 Each Accident $100,000 Each Employee by Disease $500,000 Aggregate Disease.	
Privacy and Security Liability (Cyber Liability) Insurance	
Minimal Limits: $1,000,000 Each Claim for Wrongful Acts $1,000,000 Annual Aggregate	Contractor must have their policy: cover information security and privacy liability, privacy notification costs, regulatory defense and penalties, and website media content liability. This coverage

	may be included within Agency's Professional/Errors and Omissions Liability insurance
Professional Liability (Errors and Omissions) Insurance	
Minimal Limits: $2,000,000 Each Claim $2,000,000 Annual Aggregate	

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

Contractor must: (a) provide industry standard ACORD insurance certificates to the Contract Administrator, containing the agreement or purchase order number, at Contract formation and within 20 calendar days of the expiration date of the applicable policies; (b) require that subcontractors maintain the required insurances contained in this Section; (c) notify the Contract Administrator within 10 Business Days if any insurance is cancelled in the event replacement insurance coverage meeting all of the requirements and specifications herein cannot be obtained; and (d) waive all rights against the State for damages covered by insurance. Failure to maintain the required insurance does not limit this waiver.

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

7. **Administrative Fee and Reporting.** Contractor must pay an administrative fee of 1% on all payments made to Contractor under the Contract including transactions with the State (including its departments, divisions, agencies, offices, and commissions), MiDEAL members, and other states (including governmental subdivisions and authorized entities). Administrative fee payments must be made by check payable to the State of Michigan and mailed to:

   Department of Technology, Management and Budget
   Financial Services – Cashier Unit
   Lewis Cass Building
   320 South Walnut St.
   P.O. Box 30681
   Lansing, MI 48909

   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 DTMB-Procurement.

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

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

If extended, Contractor must supply all Services at the established Contract prices and terms. The State reserves the right to 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.

9. **Independent Contractor.** Contractor is an independent contractor and assumes all rights, obligations and liabilities set forth in this Contract. 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.

a. **Intellectual Property Rights**. With the exception of Background Technology, Contractor hereby acknowledges that the State is and will be the sole and exclusive owner of all right, title, and interest in the Deliverables and all associated intellectual property rights, if any. With the exception of Background Technology, such Deliverables are works made for hire as defined in Section 101 of the Copyright Act of 1976. With the exception of Background Technology, to the extent any Deliverables and related intellectual property do not qualify as works made for hire under the Copyright Act, Contractor will, and hereby does, immediately on its creation, assign, transfer and otherwise convey to the State, irrevocably and in perpetuity, throughout the universe, all right, title and interest in and to the Deliverables, including all intellectual property rights therein.

b. "**Background Technology**" means all software, data, know-how, ideas, methodologies, specifications, and other technology in which Contractor or its subcontracts owns such Intellectual property rights as are necessary for Contractor to grant the rights and licenses set forth in this Section, and for the State (including its licensees, successors and assigns) to exercise such rights and licenses, without violating any right of any third party or any law or incurring any payment obligation to any third party. Background Technology must: (a) be identified as Background Technology in the applicable Statement of Work; and (b) have been developed or otherwise acquired by Contractor prior to the date of the applicable Statement of Work, or have been developed by Contractor outside of its performance under the applicable Statement of Work. Background Technology will also include any general consulting tool or methodology created by Contractor, which will not be required to be identified in the applicable Statement of Work.

c. Contractor hereby grants to the State such rights and licenses with respect to the Background Technology that will allow the State to use and otherwise exploit perpetually throughout the universe for its business uses the Deliverables, without incurring any fees or costs to Contractor (other than the fees set forth under this Contract) or any other Person in respect of the Background Technology. In furtherance of the foregoing, such rights and licenses will:

i. be non-exclusive, non-transferrable, non-sublicensable, irrevocable, perpetual, fully paid-up and royalty-free;

ii. include the rights for State contractors to use the Background Technology for the State's business uses; and

iii. include the rights to use, reproduce, perform (publicly or otherwise), display (publicly or otherwise), modify, improve, create Derivative Works of, import, make, and have made, the Background Technology, including all such modifications, improvements and derivative works thereof, solely as part of, or as necessary to use the Deliverables.

10. **Assignment.** Contractor may not assign this Contract to any other party without the prior written approval of the State. However, Contractor may assign the Contract to an affiliate so long as (a) Contractor provides the State thirty (30) days prior written notice of such assignment, (b) the affiliate is adequately capitalized and can provide adequate assurances that the affiliate can perform the Contract and applicable Statement of Work, and (c) a Change Notice will be executed by the parties if necessary under DTMB contracting policies. 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 Michigan state governmental entity.

11. **Change of Control.** Contractor will notify, at least 90 calendar days before the effective date, the State 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.

12. **Acceptance.** Unless otherwise provided in the applicable Statement of Work, this Section shall control acceptance ("Acceptance") of all Deliverables. Deliverables are subject to inspection and testing by the State within 30 calendar days of the State's receipt of them, or such other period as may be set forth in the applicable Statement of Work ("**State Review Period**"). If the Deliverables contain Non-Conformities, the State will notify Contractor by the end of the State Review Period that either: (a) the Deliverables are Accepted, but noted Non-Conformities must be corrected; or (b) the Deliverables are rejected. If the State finds Non-Conformities, it may: (i) reject the Deliverables without performing any further inspections if the Acceptance tests identify any Non-Conformities in such Deliverable after a second or subsequent delivery of such Deliverable; (ii) demand such Deliverables without Non-Conformities at no additional cost; or (iii) terminate a Statement of Work in accordance with **Section 15**, Termination for Cause if the Acceptance tests identify any Non-Conformities in such Deliverables after a second or subsequent delivery of such Deliverable. If the State finds no Non-Conformities in the applicable Deliverable, the State will notify the Contractor of such finding within the State Review Period.

Within 10 Business Days from the date of Contractor's receipt of notification of acceptance with Non-Conformities or rejection of any Deliverables, Contractor must cure, at no additional cost, the Non-Conformities and deliver Deliverables to the State without such Non-Conformities. The State will then have 10 Business Days, or such other period as maybe set forth in the applicable Statement of Work to inspect and test the Deliverables as described above ("Subsequent State Review Period"). If Acceptance with Non-Conformities or rejection of the Deliverables impacts the content or delivery of other non-completed Services or Deliverables, the parties' must determine an agreed to number of days for re-submission that minimizes the overall impact to the Contract. However, nothing herein affects, alters, or relieves Contractor of its obligations to correct Non-Conformities in accordance with the time response standards set forth in this Contract. The process of review as set forth in this Section shall be repeated until Acceptance occurs as described in this Section. The Deliverables will be deemed Accepted by the State hereunder if the State has not notified Contractor of one or more Non-Conformities prior to the end of the State Review Period or Subsequent State Review Period.

If Contractor is unable or refuses to correct the Non-Conformity within the time response standards set forth in this Contract after a second or subsequent delivery of such Deliverable, the State may terminate the applicable Statement of Work in whole or in part.

"**Non-Conformity**" means any failure of any: Deliverables to materially conform to the requirements of this Contract (including the applicable Statement of Work).

13. **Terms of Payment.** Invoices must conform to the requirements set forth in a Statement of Work. All undisputed amounts (as described below) are payable within 45 days of the State's receipt. Contractor may only charge for Services and Deliverables performed as specified in the applicable Statement of Work. Invoices must include an itemized statement of all charges. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Services and Deliverables purchased under this Contract are for the State's exclusive use. Notwithstanding the foregoing, all prices are inclusive 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.

The State may withhold from payment any amount disputed by the State in good faith, pending resolution of the dispute, provided that the State:

timely pays all amounts not subject to dispute;

notifies Contractor of the dispute prior to the due date, specifying in such notice (i) the amount in dispute, and (ii) the reason for the dispute set out in sufficient detail to facilitate investigation by Contractor and resolution by the parties;

works with Contractor to resolve the dispute promptly through the Dispute Resolution Procedure; and

promptly pays any amount determined to be due by resolution of the dispute.

Payment by the State will not constitute a waiver of any rights as to Contractor's continuing obligations, including claims for deficiencies or substandard Services or 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.

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.

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 the applicable Statement of Work.

14. **Stop Work Order.** The State may suspend any or all activities under at a Statement of Work at any time. The State will provide Contractor a written stop work order detailing the suspension for up to thirty (30) calendar days at no additional cost to the State. (a "**Stop Work Order**"). Contractor must comply with the Stop Work Order upon receipt.

Within 30 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 applicable Statement of Work. The State will not pay for Services or Deliverables, Contractor's lost profits, or any additional compensation during a stop work period. The parties will agree upon an equitable adjustment through the Change Control Process to (i) extend the milestone dates under the applicable Statement of Work, and (ii) adjust Contractor staffing requirements**,** if as a result of the Stop Work Order, Contractor is unable to timely meet all or any remaining milestones under the applicable Statement of Work or its staffing of the project is affected by such Stop Work Order. Notwithstanding anything contained in this Section, Contractor shall use its commercially reasonable efforts to meet the milestone dates specified in the applicable Statement of Work without any extension.

15. **Termination for Cause.** The State may terminate this Contract for cause, in whole or in part (including individuals Statements of Work), if Contractor: (a) endangers the integrity or security of any State data and fails to cure this endangerment, if curable, within ten (10) days thereafter, (b) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor; or (c) breaches any of its material duties or obligations under this Contract and fails to cure a breach within thirty (30) days of the written notice of breach. Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.

If the State terminates this Contract under this Section, the State will issue a termination notice specifying whether Contractor must: (a) cease performance immediately, or (b) continue to perform for a specified period. If it is later determined that Contractor was not in breach of the Contract, the termination will be deemed to have been a Termination for Convenience, effective as of the same date, and the rights and obligations of the parties will be limited to those provided in **Section 16**, Termination for Convenience.

The State will only pay for amounts due to Contractor for Services and Deliverables accepted by the State on or before the date of termination, subject to the State's right to set off any amounts owed by the Contractor for the State's reasonable costs in terminating this Contract. The Contractor must pay all reasonable costs incurred by the State in terminating this Contract for cause, including administrative costs, attorneys' fees, court costs, transition costs, and any costs the State incurs to procure the Services and Deliverables from other sources, subject to the limitation of liability set forth in Section 19.

Termination by Contractor. If the State breaches a material provision of this Contract, then the Contractor will provide the State with written notice of the breach and a time period (not less than thirty (30) calendar days) to cure the breach. The Contractor may terminate this Contract if the State (i) materially breaches its obligation to pay the Contractor undisputed amounts due and owing under this Contract, (ii) breaches its other obligations under this Contract to an extent that makes it impossible or commercially impractical for the Contractor to perform the Services, or (iii) does not cure the material breach within the time period specified in a written notice of breach.

16. **Termination for Convenience.** The State may immediately terminate this contract due to non-appropriation or budget shortfalls. The State may terminate this Contract upon thirty (30) days written notice, in whole or in part (including individual Statement of Work), without penalty and for any reason other than non-appropriation or budget shortfalls. The termination notice will specify whether Contractor must: (a) cease performance of the Services immediately, or (b) continue to perform the Services in accordance with **Section 17**, Transition Responsibilities. 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. Also, if the State terminates this Contract for convenience or any reason other than non-appropriation or budget shortfalls, the State will pay for all (a) accepted Deliverables, (b) work in process on a pro rata basis, and (c) any holdbacks retained by the State that are associated with already accepted Deliverables. Notwithstanding the foregoing, if the State terminates this Contract for non-appropriation, the State will pay the Contractor in accordance with applicable law. Future payments on any continuing amounts due will be made if funds become available through later appropriations, as required by MCL 17.52.

17. **Transition Responsibilities.** Upon termination or expiration of this Contract for any reason, Contractor must, for a period of time specified by the State (not to exceed 60 calendar days), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Services to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Services to the State or its designees. Such transition assistance may include, but is not limited to: (a) continuing to perform the Services at the established Contract rates (on a fixed price or time and material basis, depending on the Services provided); (b) taking all reasonable and necessary measures to transition performance of the work, including all applicable Services, training, reports and other documentation, to the

State or the State's designee; (c) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, or return to the State all materials, data, property, and confidential information provided directly or indirectly to Contractor by any entity, agent, vendor, or employee of the State; (d) transferring title in and delivering to the State, at the State's discretion, all completed or partially completed Deliverables prepared under this Contract as of the Contract termination date provided Contractor has received full payment for such Deliverable; and (e) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts (collectively, "**Transition Responsibilities**"). This Contract will automatically be extended through the end of the transition period.

18. **General Indemnification.** Contractor must defend, indemnify and hold the State, its departments, divisions, agencies, offices, commissions, officers, and employees harmless, without limitation, from and against any and all losses, liabilities, damages, reasonable costs, reasonable attorney fees, and expenses (including those required to establish the right to indemnification), to the extent arising out of third party claims or actions of or relating to: (a) any infringement, misappropriation, or other violation of any intellectual property right of any third party in connection with any Services or Deliverable provided pursuant to the Contract; and (b) any bodily injury, death, or damage to real or tangible personal property occurring wholly or in part due to negligent or more culpable 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).

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: (i) regular updates on proceeding status; (ii) participate in the defense of the proceeding; and (iii) employ its own counsel. Contractor will not, without the State's 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. To the extent that any State employee, official, or law may be involved or challenged, the State may, at its own expense, control the defense of that portion of the claim.

Any litigation activity on behalf of the State, or any of its subdivisions under this Section, 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.

(a) **Infringement Remedies.** If any of the Services or Deliverables supplied by Contractor or its subcontractors, or its operation, use or reproduction, is likely to become the subject of a copyright, patent, trademark, or trade secret infringement claim, Contractor must, at its expense: (a) procure for the State the right to continue using the Services or Deliverables, or if this option is not reasonably available to Contractor, (b) replace or modify the same so that it becomes non-infringing; or (c) accept its return by the State with appropriate credits to the State against Contractor's charges. Contractor will have no liability for any claim of infringement arising solely from:

Use of the Services or Deliverables for other than its intended use, as reflected in the Contract or documentation;

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

Modification of the Services or Deliverables by the State without the prior knowledge and approval of Contractor; or

Failure to use modifications or enhancements made available at no cost to the State by Contractor, provided Contractor has given the State written notice of such modification or enhancement, and such modification or enhancement will not degrade the Services or Deliverables performance,

unless the claim arose against the Services or Deliverables independently of any of the above specified actions.

19. **Limitation of Liability.** NEITHER PARTY 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. IN NO EVENT WILL EITHER PARTY'S AGGREGATE LIABILITY TO THE OTHER UNDER THIS CONTRACT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT, EXCEED THE MAXIMUM AMOUNT OF FEES SPECIFIED IN THE APPLICABLE STATEMENT OF WORK.

i. Exceptions. The Limitation of Liability above, shall not apply to:

1. Contractor's obligation to indemnify under **Section 18** of this Contract**;**

2. Contractor's obligations under **Section 20.C** of this Contract (Compromise of State Data), subject to the Security Breach Indemnity Cap; and

3. damages arising from either party's recklessness, bad faith, or intentional misconduct.

20. **State Data.**

a. Ownership. The State's data ("**State Data**," which will be treated by Contractor as Confidential Information) includes the State's data collected, used, processed, stored, or generated as the result of the Services. State Data is and will remain the sole and exclusive property of the State and all right, title, and interest in the same is reserved by the State. This Section survives the termination of this Contract.

b. 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 confidence, using such degree of care as is appropriate and consistent with its obligations as further described in this Contract and applicable law to avoid unauthorized access, use, disclosure, or loss; (b) use and disclose State Data solely and exclusively for the purpose of providing the Services, such use and disclosure being in accordance with this Contract, the applicable Statement of Work, and applicable law; and (c) not use, sell, rent, transfer, distribute, or otherwise disclose or make available State Data for Contractor's own purposes or for the benefit of anyone other than the State without the State's prior written consent. This Section survives the termination of this Contract.

c. Compromise of State Data. In the event of any Contractor act, error or omission, negligence, misconduct, or breach by the Contractor that compromises the security, confidentiality, or integrity of State Data or the physical, technical, administrative, or organizational safeguards put in place by Contractor that relate to the protection of the security, confidentiality, or integrity of State Data during the term of this Contract, Contractor must, as applicable: (a) notify the State as soon as practicable but no later than one (1) business day of becoming aware of such occurrence; (b) cooperate with the State in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by the State; (c) perform or take any other actions required to comply with applicable law as a result of the occurrence; (d) reimburse the State for all reasonable costs incurred by the State in the investigation and remediation of such occurrence, including but not limited to all legal fees, any audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the occurrence; and (e) without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless the State for any and all third party claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the Contractor's breach of this Section. Notwithstanding anything to the contrary set forth in this Section or any other provision of this Contract, the aggregate liability of Contractor for damages under this Section shall not exceed (i) for Statements of Work where the maximum amount of fees specified is less than $1 million ($1,000,000), the maximum amount of fees specified in the applicable Statement of Work, or (ii) for Statements of Work where the maximum amount of fees specified is greater than or equal to $1 million ($1,000,000), $2 million ($2,000,000) (the "**Security Breach Indemnity Cap**").

21. **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. The provisions of this Section survive the termination of this Contract.

   a. <u>Meaning of Confidential Information</u>. 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 or is: (a) subject to disclosure under the Michigan Freedom of Information Act (FOIA) by the receiving party; (b) already in the possession of the receiving party without an obligation of confidentiality; (c) developed independently by the receiving party, as demonstrated by the receiving party, without violating the disclosing party's proprietary rights; (d) obtained from a source other than the disclosing party without an obligation of confidentiality; or, (e) publicly available when received, or thereafter became publicly available (other than through any unauthorized disclosure by, through, or on behalf of, the receiving party). For purposes of this Contract, in all cases and for all matters, State Data is deemed to be Confidential Information.

   b. <u>Obligation of Confidentiality</u>. The parties agree to hold all Confidential Information in 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 a subcontractor is permissible where: (a) use of a subcontractor is authorized under this Contract; (b) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the subcontractor's responsibilities; (c) Contractor obligates the subcontractor in a written contract to maintain the State's Confidential Information in confidence; (d) as permitted under the applicable Statement of Work; and (e) as required by law, regulation or court order, provided that to the extent a receiving party is required to disclose confidential information pursuant to this subsection, Contractor shall provide the State with notice of the legal request within one (1) Business Day of receipt. The State shall provide Contractor with notice of the legal request as soon as possible, but in any event no later than forty-eight (48) hours prior to the due date for response. The receiving party shall assist the furnishing party in resisting or limiting the scope of the disclosure as reasonably requested by the furnishing party, to the extent permitted by law or the ability to make a colorable argument against disclosure. At the State's request, any employee of Contractor or any subcontractor who is performing Services under this Contract may be required to execute a separate agreement to be bound by the provisions of this Section.

c. Cooperation to Prevent Disclosure of Confidential Information. Each party must use its reasonable 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 promptly 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 Section **21** and each party will cooperate with the other party in seeking injunctive or other equitable relief against any such person.

d. 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.

e. Surrender of Confidential Information upon Termination. Upon termination of this Contract or a Statement of Work, in whole or in part, each party must, within 5 calendar days from the date of termination, return to the other party any and all Confidential Information received from the other party, or created or received by a party on behalf of the other party, which are in such party's possession, custody, or control. Should Contractor or the State determine that the return of any Confidential Information is not feasible, such party must destroy the Confidential Information and must certify the same in writing within 5 calendar days from the date of termination to the other party. Notwithstanding anything herein to the contrary, Contractor shall have the right to retain copies of Confidential Information, and any summaries, analyses, notes, or extracts prepared by Contractor which are based on or contain portions of such Confidential Information to the extent necessary to evidence performance of the Services, provided that Contractor retains such copies in accordance with its confidentiality obligations hereunder.

22. **Data Privacy and Information Security**. Without limiting Contractor's obligation of confidentiality as further described, Contractor is responsible for establishing and maintaining a data privacy and information security program, including physical, technical, administrative, and organizational safeguards, that is designed to: (a) ensure the security and confidentiality of State Data; (b) protect against any anticipated threats or hazards to the security or confidentiality of State Data; (c) protect against unauthorized disclosure, access to, or use of State Data; (d) ensure the proper disposal of State Data; and (e) ensure that all employees, agents, and subcontractors of Contractor, if any, comply with all of the foregoing. 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, and Contractor must at all times comply with all applicable State IT policies and standards, which are available at http://www.michigan.gov/dtmb/0,4568,7-150-56355_56579_56755---,00.html .

23. **Records Maintenance, Inspection, Examination, and Audit.** Upon written notice to Contractor, 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 the Contract through the term of the 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.

Within 10 calendar days of providing written 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 the 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 the Contract must be paid or refunded within 45 calendar days.

This Section applies to Contractor, any parent, affiliate, or subsidiary organization of Contractor, and any subcontractor that performs Services in connection with this Contract.

24. **Warranties and Representations.** Contractor represents and warrants to the State that: (a) the Services and Deliverables provided by Contractor will not knowingly infringe the patent, trademark, copyright, trade secret, or other proprietary rights of any third party; (c) it has the full right, power, and authority to enter into this Contract, to grant the rights granted under this Contract, and to perform its contractual obligations; (d) to Contractor's knowledge, all information furnished and representations made in connection with the award of this Contract is true, accurate, and complete, and contains no false statements or omits any fact that would make the information misleading; and (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. A material breach of this Section is considered a material breach of this Contract, which entitles the State to terminate this Contract under **Section 15**, Termination for Cause. TO THE EXTENT PERMITTED BY LAW, THE CONTRACTOR EXPRESSLY DISCLAIMS ANY WARRANTIES NOT LISTED HEREIN

25. **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; 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 subcontractor that performs Services in connection with this Contract.

26. **Compliance with Laws.** Contractor must comply with all federal, state and local laws, rules and regulations.

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

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

29. **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 Michigan Court of Claims. Contractor consents to venue in Ingham County, and waives any objections, such as lack of personal jurisdiction or *forum non conveniens*. Contractor must appoint agents in Michigan to receive service of process.

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

31. **Force Majeure.** Neither party will be in breach of this Contract because of any failure arising from any disaster or acts of god that are beyond their control and without their fault or negligence. Each party will use commercially reasonable efforts to resume performance. Contractor will not be relieved of a breach or delay caused by its subcontractors. If immediate performance is necessary to ensure public health and safety, the State may immediately contract with a third party.

32. **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 Project 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 15 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 15 Business Days. The parties are not prohibited from instituting formal proceedings: (a) to avoid the expiration of statute of limitations period; (b) to preserve a superior position with respect to creditors; or (c) where a party makes a determination that a temporary restraining order or other injunctive relief is the only adequate remedy. This Section does not limit the State's right to terminate the Contract.

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

34. **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.

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

36. **Survival.** The provisions of this Contract that impose continuing obligations which are intended by their nature to extend beyond the termination of the Contract will survive the expiration or termination of this Contract.

37. **Entire Agreement.** This Contract, including Statements of Work, constitutes the sole and entire agreement of the parties to this Contract with respect to the subject matter contained herein, and supersedes all prior and contemporaneous understandings and agreements, both written and oral, with respect to such subject matter. In the event of any conflict between the terms of this Contract and those of any Statement of Work or other document, the following order of precedence governs: (a) first, this Contract; and (b) second, an individual Statement of Work as of the Effective Date of that Statement of Work. NO TERMS ON CONTRACTOR'S INVOICES, WEBSITE, BROWSE-WRAP, SHRINK-WRAP, CLICK-WRAP OR OTHER NON-NEGOTIATED TERMS AND CONDITIONS PROVIDED WITH ANY OF THE SERVICES, OR DOCUMENTATION HEREUNDER WILL CONSTITUTE A PART OR AMENDMENT OF THIS CONTRACT OR IS BINDING ON THE STATE FOR ANY PURPOSE. ALL SUCH OTHER TERMS AND CONDITIONS HAVE NO FORCE AND EFFECT AND ARE DEEMED REJECTED BY THE STATE, EVEN IF ACCESS TO OR USE OF SUCH SERVICE OR DOCUMENTATION REQUIRES AFFIRMATIVE ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

38. **Contract Modification.** This Contract may not be amended except by signed agreement between the parties (a "**Contract Change Control Process**"). Notwithstanding the foregoing, no subsequent Statement of Work or Contract 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. The parties will agree on a more detailed Change Control Process in the project plan.

39. In addition to The State's responsibilities as set forth in a Statement of Work, The State shall cooperate with Contractor in the performance of the Services, including (i) providing Contractor with adequate working space, equipment and facilities and timely access to data, information, and personnel of the State; (ii) providing experienced and qualified personnel having appropriate skills to perform their assigned tasks and duties in a competent and timely fashion; (iii) providing a stable, fully functional system infrastructure environment which will support the Services and allow Contractor and the State to work productively; and (iv) promptly notifying Contractor of any issues, concerns or disputes with respect to the Services. With respect to the data and information provided by the State to Contractor or its subcontractors for the performance of the Services, the State shall have all rights required to provide such data and information,

and shall do so only in accordance with applicable law and with any procedures agreed upon in writing. Contractor’s performance is dependent upon the State’s timely and effective satisfaction of the State’s responsibilities under this Contract and any Statement of Work and timely decisions and approvals of the State in connection with the Services.

SCHEDULE A
STATEMENT OF WORK

1. Background and Scope

The Department of Technology, Management and Budget (DTMB) is executing this contract to conduct work to identify and remediate vulnerabilities through application scanning, remediation and validation of commercial and internally developed applications supporting multiple platforms and technology. The Contractor must meet the following project objectives:

a. Establish and execute a formal project delivery framework with full life cycle rigor and governance.
b. Utilize the DTMB Application Security methodology – Secure Application Development Lifecycle or SADLC, or define a methodology, of equal or more advanced to the DTMB methodology, to be followed for all in scope applications.
c. Develop remediation plans, timelines, resource plans.
d. Remediate (for applications the State has access to source code for) or suggest remediation or configuration options (for 3rd party controlled applications) to address high and medium rated vulnerabilities for in-scope applications from vulnerabilities discovered with the agreed to scanning tool(s).

The State acknowledges that the scope of Contractor's project activities does not include handling of any protected health information (PHI), personally identifiable information (PII), and/or payment card information (PCI) within the existing systems or applications in the scope of this project.

2. Project Management

Enterprise Project Management Office (EPMO) SUITE Process

Contractor must follow the EPMO standard State Unified Information Technology Environment (SUITE) process or obtain prior State approval to implement modifications. SUITE is a project management methodology used by the State of Michigan.

3. Project Charter and Project Plan

Contractor will develop and work with the State project manager to obtain State approval of a detailed project plan and charter within 30 calendar days from the date both parties execute the contract. Contractor will complete this project plan in parallel to the remediation and validation efforts of the 15 applications identified under this initial statement of work. Once approved by the State, Contractor will socialize the project plan and charter with State stakeholders. Contractor's Project Manager, Mark Wireman, will maintain the project plan and review with the State in the weekly status meetings identified in Section 12 (a). Meetings.

a. **Project Charter** will include the organizational structure of the project delivery team with clear delineation of the responsibilities and the reporting relationships between Contractor and State teams.

b. **Project Plan** will be used to track the progress and status of the project and associated deliverables and must include, but not be limited to, the following:

   i. Breakdown showing the detailed listing of all the activities that will be performed as part of the project including the project phases, sub-projects, tasks, resources, deliverables and timelines required to fully complete all remediation and validation efforts. Detailed tasks for remediation, testing and validation exercises will also be included in the project plan. The activities will be accompanied by supplementary details such as the resources performing the activities, the deliverables associated with the activities, the proposed start and end dates of the activities, etc. at a minimum.

4. Approach to Application Scanning, Remediation, and Validation

For each application to be remediated and validated the State and Contractor will complete the following:

Task and Timing	**Milestones and Deliverables**
Task 1 – Application Scanning, Deconstruction, and Vulnerability Identification Timing: Completed within 2 weeks of engagement start Owner: State	The State will dynamically or statically scan all applications utilizing the DTMB Enterprise Application Scanning platform – IBM AppScan to identify vulnerabilities. If another method of testing is required to ascertain the root cause of vulnerabilities, the State will determine if additional testing tools will be used.
Task 2 – Vulnerability Analysis and Remediation Work Plan Timing: 3 weeks from contact execution date Owner: Contractor and State	The State's central scanning function will provide application architecture and design, dynamic application security testing ("DAST") results, manual penetration testing results, and static application security testing ("SAST") analysis results. The State will reconcile findings and create a definitive prioritized list of vulnerabilities in the order of assigned severity to be remediated. The State will provide this information to Contractor along with information describing how the application interacts with external entities; use-cases to understand how the application is used, and the identification of entry points to see where a potential attacker could interact with the application, identifying assets, i.e. items/areas that the attacker would be interested in, and identifying trust levels which represent the access rights that the application will grant to external entities. Contractor will review vulnerabilities from the State's central scanning function. The State will conduct a preliminary false positive analysis. Contractor, in conjunction with the state development team and review with state app scan team, will conduct a false positive analysis of the identified vulnerabilities and scan the code base. .

	Contractor will then develop the remediation work plan. The remediation work plan must include the following: a. Review and determine severity and priority for vulnerabilities b. Recommend vulnerabilities to be remediated c. Recommend existing compensating controls that can remediate the vulnerability d. Remediation approach, including testing procedures to analyze that security vulnerabilities have been remediated e. Risk mitigation strategy f. Tasks, dependencies, resources, timelines, etc. g. Expected results h. Identification of level of effort to remediate (see Table 1 in Pricing) and amount of time needed to remediate The Remediation Work Plan must enumerate vulnerabilities and remediation tasks across the following: Common system architecture risk areas: a. Authentication b. Session Management c. Error Handling and Logging d. Hypertext Transfer Protocol (HTTP) Security e. Malicious Controls Common application risk areas, or open web application security project ("OWASP") top ten (10): a. A1: Injection b. A2: Broken Authentication and Session Management c. A3: Cross-Site Scripting ("XSS") d. A4: Insecure Direct Object References e. A5: Security Misconfiguration f. A6: Sensitive Data Exposure g. A7: Missing Function Level Access Control h. A8: Cross Site Request Forgery ("CSRF") i. A9: Using Components and Known Vulnerabilities j. A10: Un-validated Redirects and Forwards Contractor must provide key developers and vulnerability specialists to remediate identified vulnerabilities. Contractor will only act in a coordinator role for applications where Contractor is not permitted to modify code (e.g. COTS products, or applications currently maintained by other vendors). Contractor must obtain State approval for the remediation work plan, including application type for each application. Upon State approval, Contractor will conduct project kick-off meeting with the stakeholders to communicate the remediation work plan, expectations, schedule, etc.

	Contractor will update the information in the Threat Model document and produce data flow diagrams (DFDs) for each application provided by the State, specific to the remediation activities for the identified vulnerabilities which will show the different paths through the system, highlighting the privilege boundaries, and how the remediation recommendation is providing protection against the exposed boundary based on the identified vulnerability from Task 1.
Task 3 – Remediation and Resolution Validation Report Timing: 12 weeks from contract execution date. Owner: Contractor	When available and applicable (e.g. State owned/maintained applications) the State will provide Contractor with on-demand (during business hours) access to the following: a. Code bases and ability to remediate application code b. Design documents or other relevant documents, templates and related material and ability to update design documents c. Development environment and access to promote code d. Test environments or follow a process to promote code e. Production environments or follow a process to promote code f. Application administrator console or will be provided a Subject Matter Expert/Admin g. Remote Virtual Private Network (VPN) access on a 24x7 basis to the project environment h. Key application team personnel with access and knowledge of existing policies and procedures that are relevant to this contract i. Relevant hardware, software, licenses, etc. and appropriate relate setup/maintenance/support for developing project deliverables. For applications where access to <u>all application components is available</u>: a. Perform modification to application source code in the development environment b. Perform modification to application configuration settings in the development environment c. Perform modification to infrastructure configuration settings in the development environment (in conjunction with State resources if needed) d. In conjunction with Michigan Cyber Security and Telecom, perform modification to compensating controls (i.e. Firewalls, Web Application Firewalls, Access Control) The State will promote code and configuration settings into higher environments and perform testing. For applications where access to <u>one or more application components is not available</u>: a. Provide guidance and remediation assistance to each respective application development team to remediate vulnerabilities associated with the source code.

b. Provide guidance and assistance to the appropriate application architecture/infrastructure teams to remediate system configuration related vulnerabilities.

For system/architecture vulnerabilities, Contractor will complete the following:

a. Recommend and coordinate configuration changes and other compensating controls at the system/architecture level to address vulnerabilities across the in-scope applications.
b. Recommend and coordinate additional remaining configuration changes and other compensating controls at the system/architecture level specific to one or more of the in-scope applications.
c. The State will implement agreed upon configuration changes.

For application specific vulnerabilities, Contractor will complete the following tasks where applicable:

a. In coordination with each of the development teams, implement code changes or mitigating controls to address the identified vulnerabilities.
b. Assist the application development team for reviewing software source code to identify code modifications required to remediate identified vulnerabilities in the in-scope applications.
c. Assist in remediating identified vulnerabilities in software source code.
d. Review and assess original source code from the application team's version control system.
e. Modify source code to resolve identified vulnerabilities, based on approval and review of requirements and criteria by application team's personnel.
   - Submit source code changes to application team's version control system.
   - Perform remediation of application code to the in-scope applications.
   - Whenever possible, use standard, repeatable code or routines to remediate vulnerabilities.
   - Provide static code analysis to the team to analyze whether the changes have addressed the identified vulnerabilities.

For all applications where a remediation plan is executed Contractor will complete the following:

a. For .NET apps:
   - Update the common .NET Developer cookbook in SharePoint
   - Add any OWASP related links to the OWASP Links library
   - Add any .NET or Microsoft related links to the .NET Links library

	• Add any .NET or Microsoft related docs to the .NET Documents library • Add any .NET or Microsoft Code in a .ZIP file with context verbiage in the .NET Secure Code Wiki b. For Java apps: • Update the Java Developer cookbook in SharePoint • Add any OWASP related links to the OWASP Links library • Add any Java related links to the Java Links library • Add any Java related docs to the Java Documents library • Add any Java Code in a .ZIP file with context verbiage in the Java Secure Code Wiki Contractor must update the State DTMB Developer Application Security Best Practice Cookbook (DASBPC), to support cross team utilization of solutions. Update to include OWASP links, specific language links and documents and upload any reusable code in WIKI pages. Contractor must provide a report describing the outcome of executing the vulnerability remediation plans ("Resolution Validation Report"). The Resolution Validation Report must include documentation of remediation activities performed and the outcomes achieved, system architecture changes and exceptions, and that the update to the DASBPC has been completed. The Resolution Validation Report will be an artifact within the Remediation Validation Report deliverable. Vulnerabilities or defects identified in commercial software products are the State's responsibility to resolve. It is the State's responsibility to install, test, and implement software patches to address vulnerabilities identified in commercial software products.
Task 4 - Retesting After Remediation Timing: Each application to be retested within two weeks of remediation performed under Task 3 Owner: State and the Contractor	After Contractor provides the State with the Resolution Validation Report, the State will re-run the scan to validate the remediation is complete and the State will determine if additional remediation efforts will be conducted. Any additional remediation efforts will follow the process identified in Section 3, Approach to Application Scanning, Remediation and Validation. Once the remediation for the agreed upon number of vulnerability types has been completed any future testing and remediation efforts would be considered out of scope and need to be handled through a change request. After completion of Task 4 and the State's approval of code changes and recommendations Contractor will have no responsibility or liability for any recommended configuration changes or custom code developed to address State identified vulnerabilities in the in-scope applications.

Task 5 - Create Backlog for Developers Timing: Within one week of each application retesting in Task 4 and 5 Owner: Contractor	After re-testing, Contractor will arrive at a reasonable set of vulnerabilities that the State will report into the Plan of Action & Milestone (POA&M) process or similar, particularly for vulnerability that may require longer resolution time. To enable this, Contractor will create a backlog into which we load all the vulnerabilities and hand it over to the developers to start the long-term process of them caring for the vulnerability management of their application.
Task 6 - Education and Cultural Change Timing: 1 day Owner: Contractor	Contractor will educate and provide a controlled set of rules and training on how to securely develop application code to be reused by the State with up to two three-hour learning sessions.

	Week													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Task 1 - Scanning	🟦	🟦												
Task 2 - Analysis	🟧	🟧	🟧											
Task 3 - Remediation			🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨		
Task 4 - Retesting					🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
Task 5 - Developer Backlog					🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪
Task 6 - Education and Culture Change										🟩				

5. Staffing

a. **Work Hours** Contractor will provide the Services during the State's normal working hours Monday – Friday 8:00 am to 5:00 pm, Eastern Standard time, and evenings and weekends. The work schedule will be determined by the State and will depend on the specific remediation efforts and potential business impact.

b. **Work Location** Lansing, MI, and as approved, some work may be performed off-site, but must be within the United States. The State will provide office space for Contractor's team.

6. State Project Contacts

Role	Name	Title
Executive Sponsor	Rajiv Das	Deputy Director and Chief Security Officer
Co-Sponsor	Rodney Davenport	Deputy Director and Chief Technology Officer
Co-Sponsor	Tiziana Galeazzi	Acting Deputy Director – Agency Services

Program Lead and Project Manager	Jose Semidei	Program Manager – MCS Contact Number **517-241-2261**

7. DTMB Application Scanning System Administrator

The State will provide Contractor with access to the DTMB Application Scanning System Administrator

8. DTMB Application and Infrastructure SME

The State will provide subject matter experts for customer and infrastructure applications.

9. State Resources

a. **Program Lead and Project Manager** The State Program Lead and Project Manager will oversee the project, make management and prioritization decisions and work side-by-side with Contractor's team. Additional responsibilities include providing support for planning, access, issue resolution, schedule workshops and meetings with the State staff and project stakeholders.

b. **Project Steering Committee** The State will establish a project steering committee to oversee the progress of the project. This steering committee will have representation from Contractor. Contractor may conduct periodic quality reviews on the services being delivered and the State wil cooperate and participate in such reviews.

10. Contractor Project Contacts

Role	Name Title
Engagement Leader Ultimate responsibility for Contractor's performance of services under this contract in addition to acting as a subject matter specialist	Mark Moore, Managing Director, Deloitte & Touche LLP
Vulnerability Specialist and Project Manager (Key Personnel and will be on site) Run the day to day activities of Contractor's project team and assist with various project management activities as well as developing the vulnerability remediation strategy for the in-scope applications.	Mark Wireman, Specialist Leader, Deloitte & Touche LLP
Senior Vulnerability Remediation Specialist Will work under Mark Wireman's direction to perform the analysis, remediation and validation tasks.	Mechelle McGowan, Senior Consultant, Deloitte & Touche LLP
Vulnerability Remediation Specialist Will work under Mark Wireman's direction to perform the analysis, remediation and validation tasks.	Specific resources to be confirmed during analysis phase of the project

Vulnerability Remediation Developers Will work under Mark Wireman's direction to perform application remediation tasks.	Specific resources to be confirmed during analysis phase of the project
Engagement Advisors Provide ongoing thought leadership on the execution methodology and analysis of lessons learned from the remediation and validation efforts, as well as provide guidance and thought leadership on how to implement security, patching, and monitoring controls throughout the State IT infrastructure. Assist the project team assimilate into the State's culture and working environment.	Mark Ford, Principal, Deloitte & Touche LLP
Engagement Advisor In addition to helping our vulnerability remediation specialists navigate and succeed at the State, will provide subject matter knowledge as needed with respect to future sustainability of control processes, ongoing monitoring of completed work, and validation of completed remediation efforts. James will also support various project management activities and identifying the best available resources to execute the remediation activities.	James Shaw, Senior Manager, Deloitte & Touche LLP

11. Contractor Key Personnel

Mark Wireman is Contractor's Project Manager who will be directly responsible for the day-to-day operations of the Contract ("Key Personnel"). Mark Wireman must be specifically assigned to the State account, be knowledgeable on the contractual requirements, and respond to State inquires, and be on-site in Lansing, MI during the normal business hours. Mark Wireman will coordinate with State application owners and project managers to plan remediation, validation and retesting activities. In addition to Mark, the Contractor team will be onsite to complete remediation, validation and retesting activities.

Contractor will provide the State, prior to the assignment to work under this contract, with resumes for all individuals performing services under this contract. Assignment of any subcontractor is subject to the requirements provided in Section 3, f of the IT Professional Services Contract Terms.

12. Meetings

a. **Weekly Team Meetings** The State and Contractor's project team will meet weekly to review and discuss, including, but not limited to the following:
   - **i.** Weekly 4-up report
   - ii. Project status and schedule
   - iii. Progress of the team
   - iv. Deliverable/work product development
   - v. Raise and discuss unresolved issues that may have an impact on project performance

Contractor’s Project Manager will facilitate the meetings, develop and circulate meeting agendas, meeting minutes and save the meeting records to the project’s document repository. Immediately following the weekly review meeting Contractor will update the project plan to reflect the current status. Contractor will provide the updated plan to the State Project Manager for approval.

The State may request other meetings, as it deems appropriate.

13. Reporting

a. **Weekly Status Reports** Contractor must provide the State Program Manager a weekly status report and monthly status report (4-up or similar) to include at a minimum the following: weekly accomplishments, planned activities, potential issues/risks, outstanding items and schedule/scope changes. The status report must be provided on the last working day of the week and Contractor must save the weekly report to the designated project document repository.

b. **Monthly Status Reports** Contractor will provide the State Program Manager a monthly status report that will provide the State with the ability to assess the health of the project and review status items, issues and risks. The status report must be provided to the State by the last working day of the month and saved in the designated project document repository.

c. **Other Reports** Other reports as identified in this contract.

14. Oath of Office

Department of Insurance and Financial Services will require Contractor and all employees and subcontractors to take an Oath of Office before beginning work. This oath ensures that employees and contractors who have access to the Department of Insurance and Financial Services regulatory information keep the information confidential.

SCHEDULE B
High Value Applications

This schedule identifies the initial 15 applications that Contractor must complete (Tasks 2-3 identified in **Section 4, Approach to Application Scanning, Remediation, and Validation)** within 60 business days following the date the State provides Contractor with the requirements of Task 1 of this same Section.

High Value Applications - derived from Red Card Apps	**Program Language**	**Platform**	**Database**	**Code maintained by DTMB or 3rd Party Vendor**	**Approx Lines of code**
Clarety (ORS Retirement System)	Java, Websphere	Client/Server Windows	SQL	DTMB Supported	700K+
OMS	.NET Framework	Web	SQL	DTMB Supported	100K
MiTEAM Fidelity	C# .NET	Web	Oracle	DTMB Supported	75K
ORS Contact Center	VoiceXML CCXML ASP JSP	Voice Platform Solution (VPS)	Microsoft SQL	DTMB / Vendor	Unknown
Integrated Service Delivery (ISD) - Contact Center	inContact SaaS	Cloud	inContact SaaS	Vendor Supported	No custom code
Bridges **"Including Universal Caseload"** Integrated Service Delivery-(ISD) - Universal Caseload-(UCL)	Java, eSQL	IIB/Websphere	Oracle	DTMB Supported	6M+
Electronic Payment Processing Information Control (EPPIC)	Java	• Red Hat Linux • Java(TM) SE Runtime Environment	Oracle	Vendor Supported and hosted	unknown
Contract Tracking Payment System (CTPS)	C# .NET	Web	Oracle	DTMB Supported	100K
MiWaters	.NET	Web	SQL SERVER	Vendor Supported	200K +
AIMS	Salesforce APEX	Salesforce Unlimited in the Govt Cloud		DTMB and Vendor Supported	67,610 lines of APEX, 764 APEX Classes, 206 APEX triggers

Electronic Death Registry System (EDRS)	Java	Web	Oracle	DTMB Supported	746,500
Life Insurance and Annuity Search (LAIS)	.Net C# (MVC)	Windows IIS	Oracle	DTMB Supported	1,000 not including libraries
Online Complaint Form	.Net C# (Web Forms)	Windows IIS	Oracle	DTMB Supported	5,500 not including libraries
Birth Registry System (BRS)	Java	Web	Oracle	DTMB Supported	500K

SCHEDULE C
Pricing

This is a fixed price contract and the pricing below include all costs, including but not limited to, any one-time or set-up charges, fees, and potential costs under this Contract.

The work under this SOW will be executed in two phases: assessment and remediation. The first phase will be to analyze the assessment results provided by the State to Contractor. The pricing for the first phase will be fixed as indicated below for the analysis of the 15 applications listed in Schedule B. During the first phase the applications will be categorized by remediation complexity level to determine the effort and pricing for the remediation phase. Complexity level will be determined using a scoring system that evaluates the effort drivers of the remediation work including: number of programming languages, lines of code, time since the most recent security assessment, application configuration type and other criteria listed below in Pricing Table 1. Application remediation will be performed on a fixed fee basis according to the complexity level and relevant assumptions.

Milestone	Deliverable	Pricing
Assessment Phase - Section 4 Task 2, Vulnerability Analysis and Remediation Work Plans	Bundled State Approved Remediation Work Plans for applications identified in Schedule B	$59,990 for 14 applications ($4285 per application)
Remediation and Validation Phase Section 4 – Tasks 3-5	Remediation Validation Report and state sign-off on Re-testing for each application	$47,000 per Complex application $36,900 per High application $27,700 per Medium application $23,100 per Low application All Remediation pricing assumes a maximum of 12 unique vulnerability types per application.
Education and Culture Change – Task 6	Development rules and training presentation document and training	No cost

Pricing for worked performed under subsequent statements of work will not exceed the pricing identified in this Statement of Work (e.g. $4285 per application for the Assessment Phase, and the prices identified for the Remediation and Validation Phase) so long as the State provides Contractor with a minimum of 15 applications for each subsequent Statement of Work.

The Task 2 deliverable will be invoiced upon approval of the Task 2 deliverable “Bundled State Approved Remediation Work Plans”.

The Task 3-5 deliverable "Remediation Validation Report and state sign-off on Re-testing for each application" will be invoiced individually at the conclusion of Task 5 for each of the 14 applications.

Total duration of the engagement is 14 weeks or 70 business days, starting on July 30, 2018. Engagement conclusion is dependent on vulnerability remediation and retesting and may result in a finish date sooner than 70 business days. Upon agreement by the State and the Contractor, the timelines may be extended.

The State will have 5 business days to approve deliverables or provide feedback. If not feedback is received after 5 business days deliverables will be considered approved. Contractor will have 5 business days to address feedback received on deliverables.

If more than 12 unique vulnerability types per application are identified and the State wishes to have Contractor fix those additional vulnerability types that work will be billed on a time and material basis according to the following rate card:

Role	**Deloitte Title**	**Hourly Rate**
Engagement Leader	Principal/Managing Director	$ 302
Project Manager	Senior Manager	$ 281
Team Lead	Manager or Solution Manager	$ 262
Vulnerability Management Sr. Specialist	Senior Consultant or Senior Solution Engineer	$ 229
Vulnerability Management Specialist	Consultant or Solution Engineer	$ 198

Pricing Table 1 – Application Remediation Complexity Scoring

	Score	Complexity Level
Infrastructure Scoring		
Fix & Config Change	2	Medium
Fix & No Config Change	1	Low
No Change	0	NIL
COTS App Scoring		
External	3	High

Non-COTS	1	Low
Custom App Scoring		
Greater than 100 modules	4	Complex
50 modules to less than 100 modules	3	High
25 to less than 50 modules	2	Medium
Less than 25 modules	1	Low
Number of Users		
Greater than 10k	4	Complex
5k to less than 10k	3	High
1k to less than 5k	2	Medium
Less than 1k	1	Low
Number of App Languages		
3 or greater languages	4	Complex
2 languages	3	High
1 language	1	Low
Number of Lines of Code		
Greater than 1 Million	4	Complex
500k to less than 1 Million	3	High
100k to less than 500k	2	Medium
Less than 100k	1	Low
Recent Security Assessment (COTS and non-COTS)		
More than 3 years or Never	4	Complex
24 months to less 3 years	3	High
12 months to less than 24 months	2	Medium
Less than 12 months	1	Low
Application Configuration (COTS and non-COTS)		
ERP or SAP	4	Complex
Non-ERP or SAP	1	Low

N-Tier	4	Complex
Non-N-Tier	1	Low
Complex	27+	
High	18+ to 27	
Medium	9 to 18	
Low	8 or less	

Invoice Requirements

All invoices submitted to the State must include: (a) date; (b) purchase order number; (c) description of the Services; (d) unit price; and (e) total price. Overtime, holiday pay, and travel expenses will not be paid.

Contractor may invoice the State monthly following the State approval of the deliverables identified above.

Travel Expenses

Travel expenses, including hotel, mileage, meals, parking, etc. are not authorized under this Contract.

Assumptions

1. Contractor will not be responsible for executing QA, Pre-Deployment, or Deployment activities upon completion of remediation activities.
2. Completed application security scans shall be immediately available and results accessible to the Contractor personnel at the start of the project.
3. Contractor will not verify or validate the efficiency of security tests executed
4. The State of Michigan will provide immediate and continued access to key personnel with access and knowledge of existing policies and procedures that are relevant to this engagement.
5. The State is responsible for organizational communication of project goals and expectation management. In addition, the State is responsible for providing appropriate points of contact (for problem escalation, reporting, etc.) in a timely manner.
6. The services will be performed in accordance with the Statement on Standards for Consulting Services issued by the American Institute of Certified Public Accountants (AICPA). We will provide our observations, advice, and recommendations. However, our services will not constitute an engagement to provide audit, compilation, review, or attestation services as described in the pronouncements on professional standards issued by the AICPA, and, therefore, we will not express an opinion or any other form of assurance with respect to the State's system of internal control over financial reporting or its compliance with laws, regulations, or other matters.
7. Up to 12 unique vulnerabilities per application are assumed for the pricing options provided. Additional vulnerabilities to be analyzed and remediated will be appropriately priced using a change order.

8. The time and materials (T&M) hourly rates for Contractor staff under this Statement of Work shall remain in place for the period of one (1) year following the date of contract execution. The T&M hourly rate corresponding to each staff will be increased by no more than five percent (5%) each year for the duration of the contract, including the possible extension years.
9. Contractor will only modify custom source code controlled by the State. Contractor will not modify commercial software products.
10. The State will be responsible for software licenses or other costs associate with tools required for vulnerability testing or remediation. (e.g. source code repository and development tools).